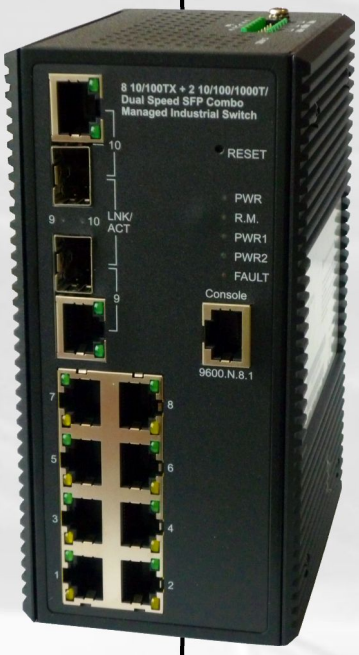
N965

Managed industrial switch



User manual

EQUITEL

About this manual …

This document is the technical reference of the model **N965**, an 8 10/100TX + 2 10/100/1000T/SFP modules combo - Managed Industrial Switch -

.

© Equipos De Telecomunicación Optoelectrónicos, S.A.
Zaragoza, Spain, Jan 2013.
Ed. 2.01

Equipos de Telecomunicación Optoelectrónicos, S.A.
Polígono de Malpica, c/ F oeste, G. Quejido, nave 74
50057 Zaragoza SPAIN
Tel. +34 976 570 353
Fax +34 976 571 383
E-mail: mail@equitel.es
www.equitel.es

The information included in this manual cannot be copied or reproduced in any way without the previous written authorisation of Equipos de Telecomunicación Optoelectrónicos, S.A.

Content

Chapter 1 Introduction 1
1.1 Hardware Features 1
1.2 Software Features 4
1.3 Package Contents 7
Chapter 2 Hardware Description 8
2.1 Physical Dimension 8
2.2 Front Panel 8
2.3 Bottom View 9
2.4 LED Indicators 10
Chapter 3 Hardware Installation 12
3.1 Installation Steps 12
3.2 DIN-Rail Mounting 13
3.3 Wall Mount Plate Mounting 15
3.4 Wiring the Power Inputs 16
3.5 Wiring the Fault Alarm Contact 17
3.6 Cabling 18
Chapter 4 Network Application 23
4.1 Pro-Ring2s Application 24
Chapter 5 Console Management 25
5.1 Connecting to the Console Port 25
5.2 Pin Assignment 25
5.3 Login in the Console Interface 26
5.4 CLI Management 28

Chapter 6 Web-Based Management 29
6.1 About Web-based Management 29
6.2 Preparing for Web Management 29
6.3 System Login 30
6.4 System 31
6.5 Time - SNTP 34
6.6 Account - Admin 37
6.7 IP Addressing – IPV4 38
6.8 Syslog 40
Syslog Configuration 40
6.9 SNMP Configuration 41
SNMP - Agent 41
6.20.1 SNMP Trap Configuration 43
6.10 System Alert - Relay Alarm 44
6.8.1 System Alert - SMTP 44
6.8.2 System Alert - Event 46
6.11 DHCP Server 48
6.6.1 DHCP Server - Server configuration 48
6.6.2 Client Table 49
6.6.3 IP Bindings 49
6.12 Port - Configuration 51
6.13 Port Status 52
6.14 Port Statistics 54
6.15 Port – Port Alert 56
6.16 Rate Control –Rate Limit 57
6.17 Aggregation - Configuration 59

6.17.1 Configuration 60
6.17.2 Aggregator – Status 62
6.18 Spanning Tree 63
6.18.1 RSTP Setting 63
6.18.2 RSTP Information 65
6.19 Pro-Ring II S 66
6.20 Multicast Support 68
6.21 LLDP 71
6.22.1 LLDP Neighbors 72
6.23 Filtering Database 73
6.24 VLAN 75
6.24.1. VLAN Configuration 75
6.24.2 Switch Status 78
6.25 QoS 79
6.25.1 Global Settings 79
6.25.2 Port Priority 80
6.25.3 COS Mapping to Queue 81
6.25.4 DSCP mapping to queue 82
6.25. Port Mirroring 84
6.26. Security 85
6.26.1 IP Source Guard - Configuration 85
6.26.2 IP Source Guard – Static Table 86
6.26.3 802.1X/Radius 87
6.26.4 MAC Filtering 91
6.26.5 Port Security 92
You can block the un-authorized MAC by oer port in this function. 92

6.27. Maintenance 93
6.27.1 Save Configuration 93
Troubles shooting 98
Appendix A—RJ-45 Pin Assignment 99
RJ-45 Pin Assignments 99
RJ-45 Pin Assignment of PoE 102
Appendix B—Command Sets 104
Switch Setting Commands Set 104
Admin Password Commands Set 105
IP Setting Commands Set 105
SNTP Commands Set 106
LLDP Commands Set 107
Backup & Restore Commands Set 108
Upgrade Firmware Commands Set 108
DHCP Server Commands Set 109
Port Control Commands Set 110
Port Status Commands Set 112
Rate Limit Commands Set 112
Trunk Commands Set 114
PRO-RING IIS Commands Set 115
RSTP Commands Set 116
VLAN Commands Set 118
SNMP Commands Set 121
Traffic Prioritization Commands Set 122
IGMP Commands Set 123
Multicast Static Filtering Table Commands Set 124
IP Security Commands Set 125

Port Security Commands Set 126
MAC Blacklist Commands Set 126
802.1x Commands Set 127
Fault Alarm Commands Set 129
System Warning Commands Set 130
Mac Address Table Commands Set 133
Port Statistics Commands Set 133
Port Monitoring Commands Set 134
System Event Log Commands Set 135
Ping Commands Set 135
SFP Monitor Commands Set 135
Loading Average Commands Set 135
Save Configuration Commands Set 137
Factory Default Commands Set 137
System Reboot Commands Set 138
Logout Commands Set 138

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Chapter 1 Introduction

The 8 10/100TX + 2 10/100/1000T/Dual Speed SFP Combo Managed Industrial Switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. Using fiber port can extend the connection distance that increases the network elasticity and performance.

1.1 Hardware Features

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/ FX IEEE802.3ab 1000Base-T IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree/ IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE802.1ab LLDP
Switch Architecture	Back-plane (Switching Fabric): 7.4Gbps Packet throughput ability(Full-Duplex): 8.3Mpps @64bytes
Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Fiber Ethernet port
Packet Buffer	1Mbits
MAC Address	8K MAC address table

Flash ROM	4Mbytes
DRAM	32Mbytes
Connector	10/100TX: 8 x ports RJ-45 with Auto MDI/MDI-X function 10/100/1000T/SFP Combo port: 2 x RJ-45 + 2 x 100/1000 SFP socket with DDM RS-232 connector: RJ-45 type
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5/ 5E cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m) 1000Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m)
Optical Fiber	Distance: Multi mode: 0 to 5 km, 1300 nm (50/125 µm, 800 MHz*km) 0 to 4 km, 1300 nm (62.5/125 µm, 500 MHz*km) Single mode: 0 to 40 km, 1310 nm (9/125 µm, 3.5 PS/(nm*km)) 0 to 80 km, 1550 nm (9/125 µm, 19 PS/(nm*km)) Min. TX Output: Multi mode: -20 dBm Single mode: 0 to 40 km, -5 dBm; 0 to 80 km, -5 dBm Max. TX Output: Multi mode: -14 dBm Single mode: 0 to 40 km, 0 dBm; 0 to 80 km, 0 dBm Sensitivity: -36 to -32 dBm (Single mode); -34 to -30 dBm (Multi mode)
Protocol	CSMA/CD

LED	Per unit: Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green), FWD (Green) 8 port 10/100: Link/Activity (Green), Full duplex/Collision (Amber) SFP port: LNK/ACT(Green), 1000T: LNK/ACT(Green), 1000M(Green)
Power Supply	External Power Supply: DC 12~48V, Redundant power DC 12~48V and connective removable terminal block for master and slave power
Power Consumption	9.86 W at full load
Operating Humidity	5% to 95% (Non-condensing)
Operating Temperature	-40°C ~ 75°C
Storage Temperature	-40°C ~ 85°C
Case Dimension	IP-30, 72mm (W) x 105mm (D) x 152mm (H)
Installation	DIN rail and wall mount ear
EMI	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4
Safety	UL, cUL, CE/EN60950-1
Stability Testing	IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock), IEC60068-2-6 (Vibration)

1.2 Software Features

Management	SNMP v1 v2c, v3/ Web/Telnet/CLI
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 , RFC 1757, RSTP MIB, Private MIB, LLDP MIB
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4094.) GVRP (256 Groups)
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
LLDP	Supports LLDP allowing switch to advertise its identification and capability on the LAN
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
Pro-Ring2s	Supports Pro-Ring2s. Provides redundant backup feature and the recovery time below 20ms
Quality of Service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”.

IGMP	Supports IGMP snooping v1,v2 256 multicast groups and IGMP query
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
Login Security	Supports IEEE802.1X Authentication/RADIUS
Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K~102400Kbps(10/100), 100K~256000Kbps(1000) Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 100K~102400Kbps(10/100), 100K~256000Kbps(1000)
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown, power fail Alarm Relay current carry ability: 1A @ DC24V
SNMP Trap	1. Topology Change 2. Power Trap 3. MAC-Violation

DHCP	Provides DHCP Client/ DHCP Server/ Port and IP Binding
DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware Update	Supports TFTP firmware update, TFTP backup and restore.
Configuration Upload/Download	Supports binary format configuration file for system quick installation
ifAlias	Each port allows importing 128bits of alphabetic string of word on SNMP and CLI interface

1.3 Package Contents

Please refer to the package content list below to verify them against the checklist.

- 8 10/100TX + 2 10/100/1000T/Dual Speed SFP Combo Managed Industrial Switch x 1
- User manual x 1
- Pluggable Terminal Block x 1
- Mounting plate x 2
- RJ-45 to DB9-Female cable x 1

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

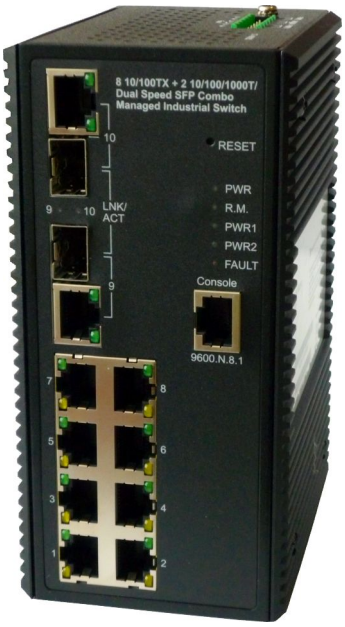
Chapter 2 Hardware Description

In this paragraph, it will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

2.1 Physical Dimension

74mm x 115mm x 152mm(W x D x H)

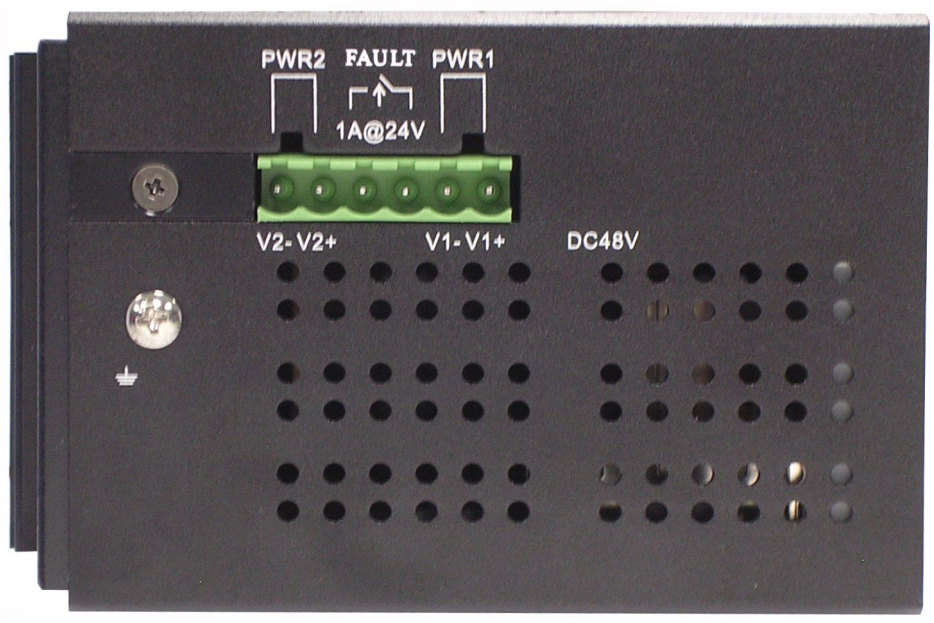
2.2 Front Panel



Front Panel of the industrial switch

2.3 Bottom View

The bottom panel of the Industrial Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.



Bottom Panel of the industrial switch

2.4 LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the industrial switch. The following table provides the description of the LED status and their meanings for the switch.

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on
		Off	No power
R.M.	Green	On	The industrial switch is the master of Pro-Ring2s group
		Off	The industrial switch is not a ring master in Pro-Ring2s group
PWR1	Green	On	Power 1 is active
		Off	Power 1 is inactive
PWR2	Green	On	Power 2 is active
		Off	Power 2 is inactive
FAULT	Red	On	Power or port failure
		Off	No failure
P9, P10 (RJ-45)	Green (Upper LED)	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Green (Lower LED)	On	1000M
		Off	10/100M

Link/Active (P9, P10 SFP)	Green	On	The SFP port is linking
		Blinks	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
P1 ~ P8	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Amber	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.
FWD (P1 ~ P8)	Green	Green	A powered device is connected utilizing Power over Ethernet on the port
		Off	No device is connected or power forwarding fails

Chapter 3 Hardware Installation

In this paragraph, we will describe how to install the Pro-Ring2s Managed Industrial Switch and the installation points attended to it.

3.1 Installation Steps

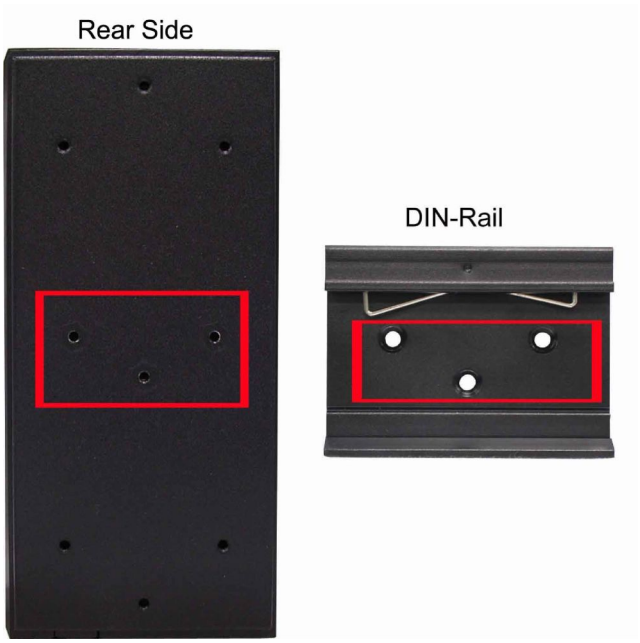
1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If users want to wall mount the Industrial switch, please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall.
4. Power on the Industrial switch. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.
6. Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

[NOTE] Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover category-5 cable.

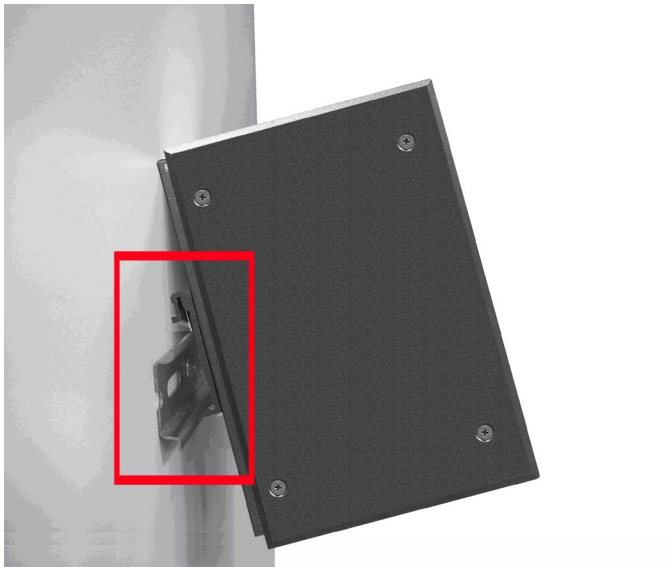
7. When all connections are set and LED lights all show in normal, the installation is complete.

3.2 DIN-Rail Mounting

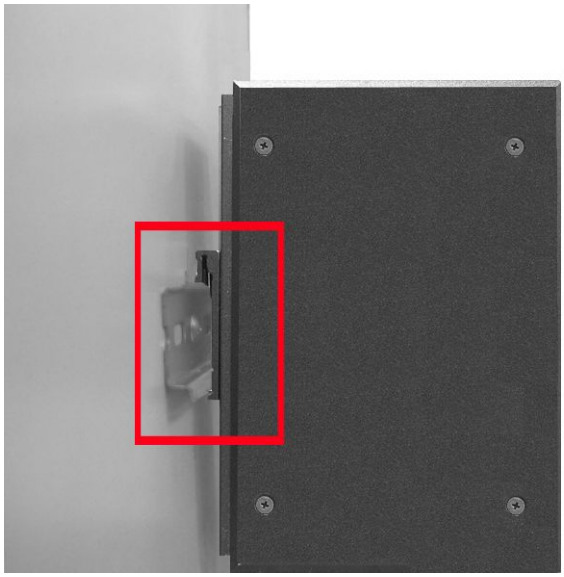
The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the steps below to hang the industrial switch.



1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

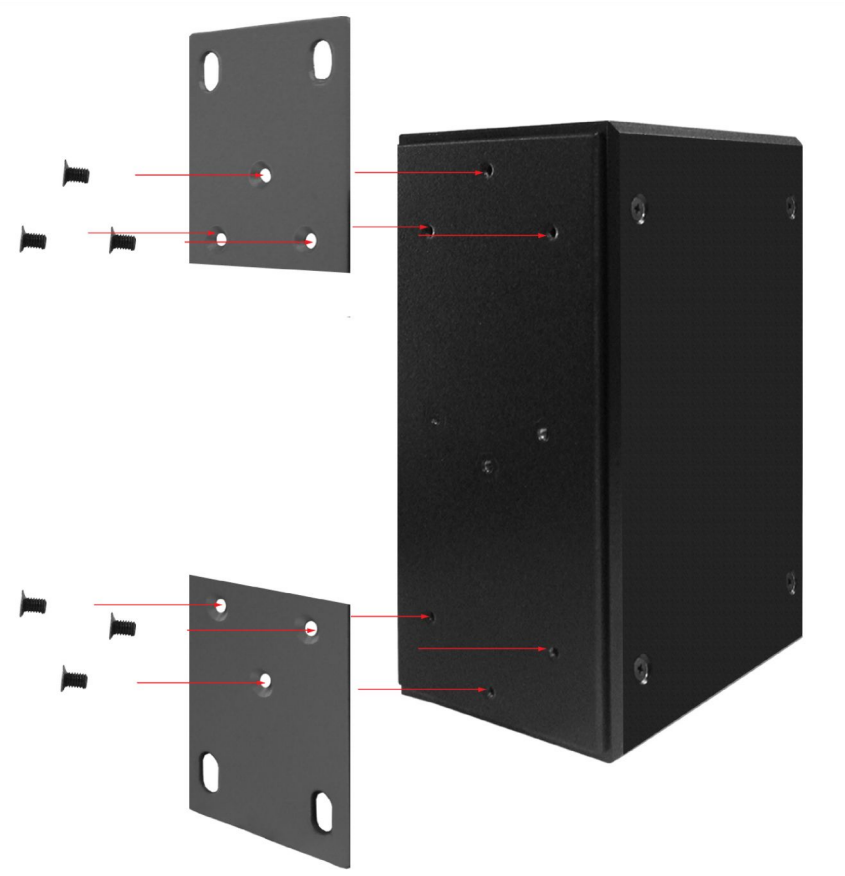


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

3.3 Wall Mount Plate Mounting

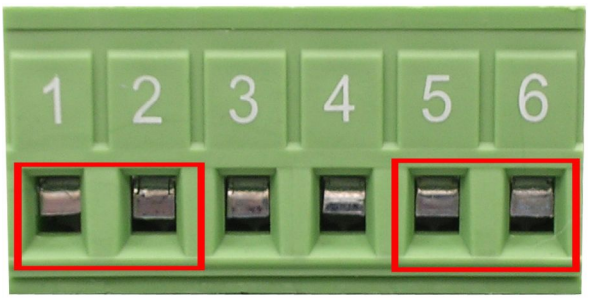
Follow the steps below to mount the industrial switch with wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to hang the industrial switch on the wall.
5. To remove the wall mount plate, reverse the above steps.

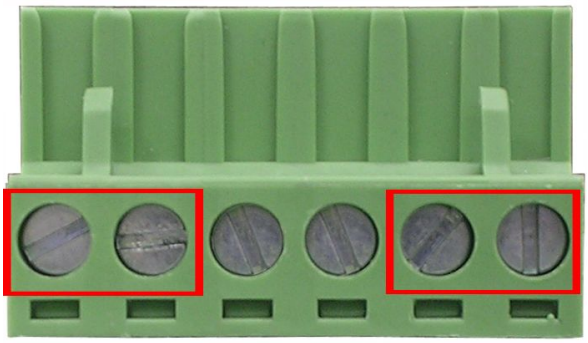


3.4 Wiring the Power Inputs

Please follow the steps below to insert the power wire.



1. Insert AC or DC power wires into the contacts 1 and 2 for power 1, or 5 and 6 for power.

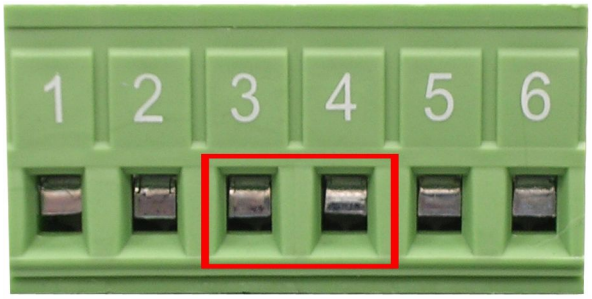


2. Tighten the wire-clamp screws for preventing the wires from loosing.

[NOTE] The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.

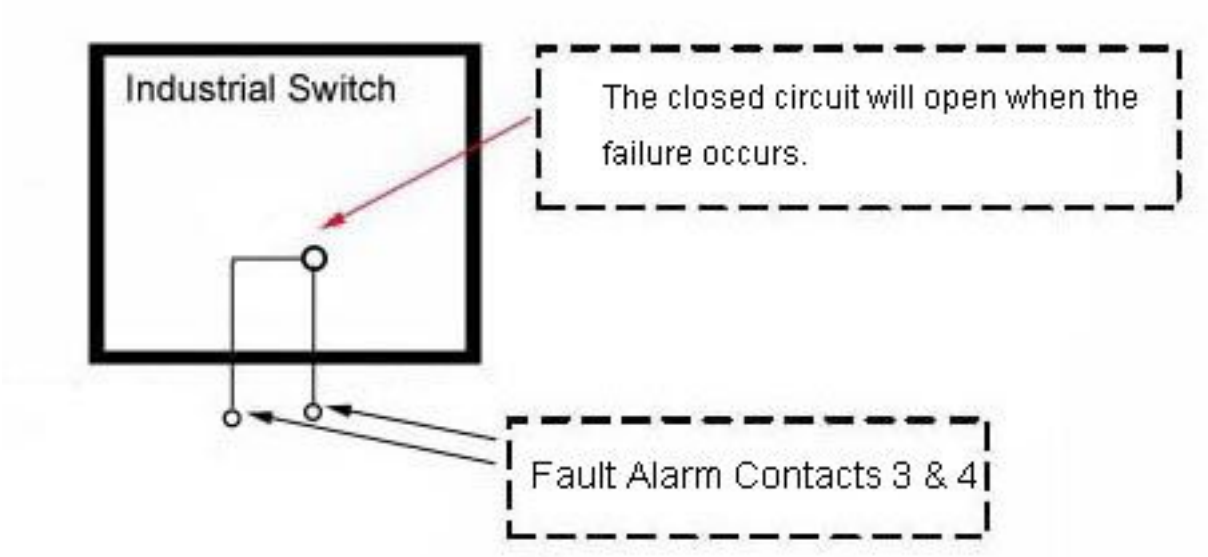
3.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the switch will detect the fault status of the power failure, or port link failure (available for managed model) and then forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.



Insert the wires into the fault alarm contacts

[NOTE] The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.



3.6 Cabling

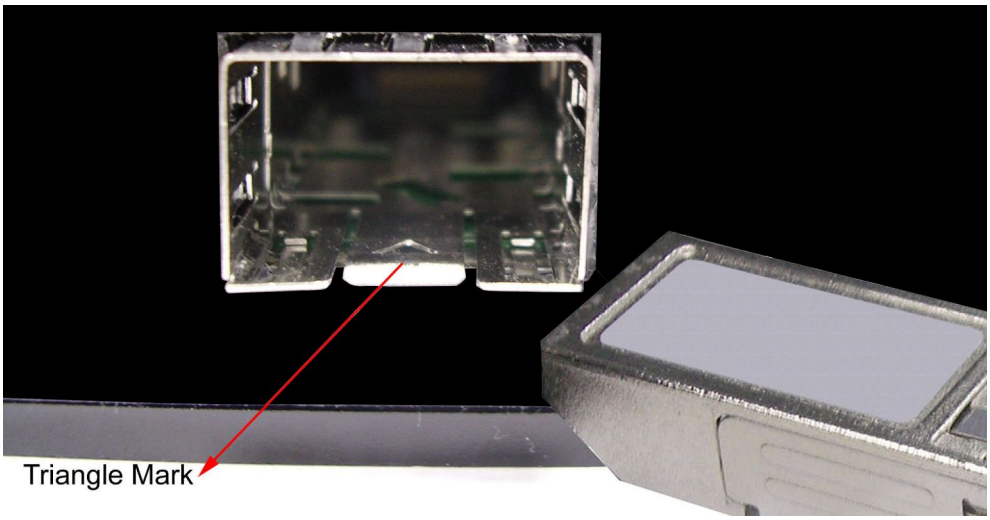
- Use four twisted-pair, Category 5e or above cabling for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segment using **single-mode** connector type must use 9/125 µm single-mode fiber cable. User can connect two devices in the distance up to **30km**.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 µm multi-mode fiber cable. User can connect two devices up to **2km** distances.
- **Gigabit Copper/SFP (mini-GBIC) combo port:**

The Industrial switch has the auto-detected Giga port—Gigabit Copper/SFP combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications. The SFP slots supporting dual mode can switch the connection speed between 100 and 1000Mbps. They are used for connecting to the network segment with single or multi-mode fiber. You can choose the appropriate SFP transceiver to plug into the slots. Then use proper multi-mode or single-mode fiber according to the transceiver. With fiber optic, it transmits at speed up to 1000 Mbps and you can prevent noise interference from the system.

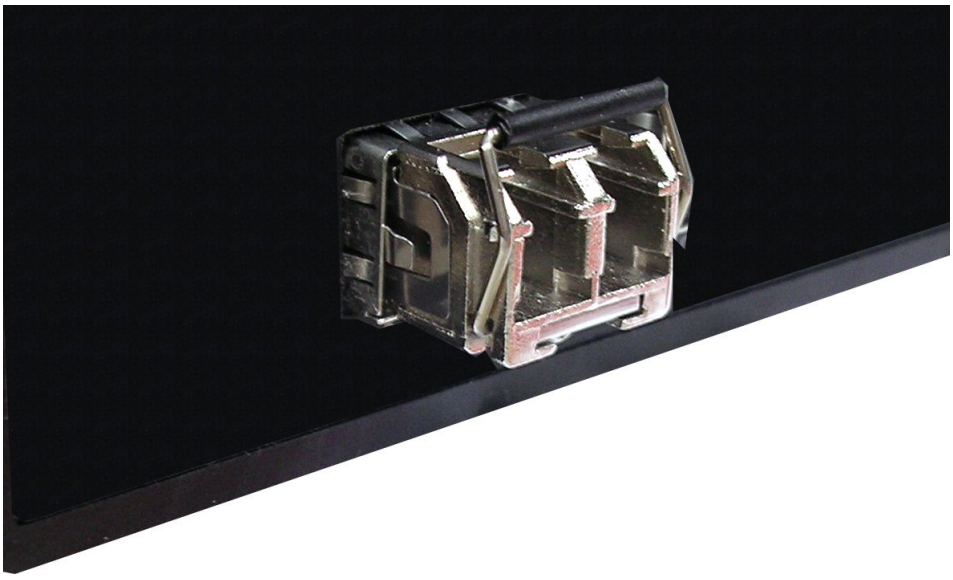
Note	*The SFP/Copper Combo port can't both work at the same time. The SFP port has the higher priority than copper port; if you insert the **1000M** SFP transceiver (which has connected to the remote device via fiber cable) into the SFP port, the connection of the accompanying copper port will link down.* *If you insert the **100M** SFP transceiver into the SFP port even without a fiber connection to the remote, the connection of the accompanying copper port will link down immediately.*

To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

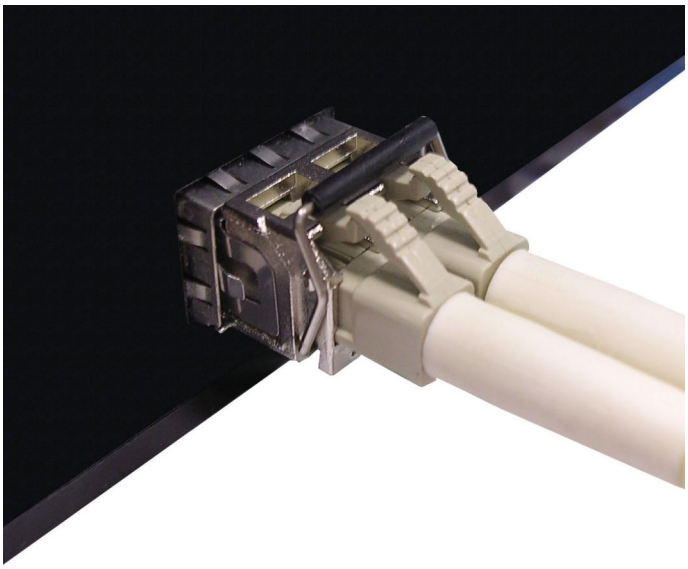


Transceiver to the SFP module



Transceiver Inserted

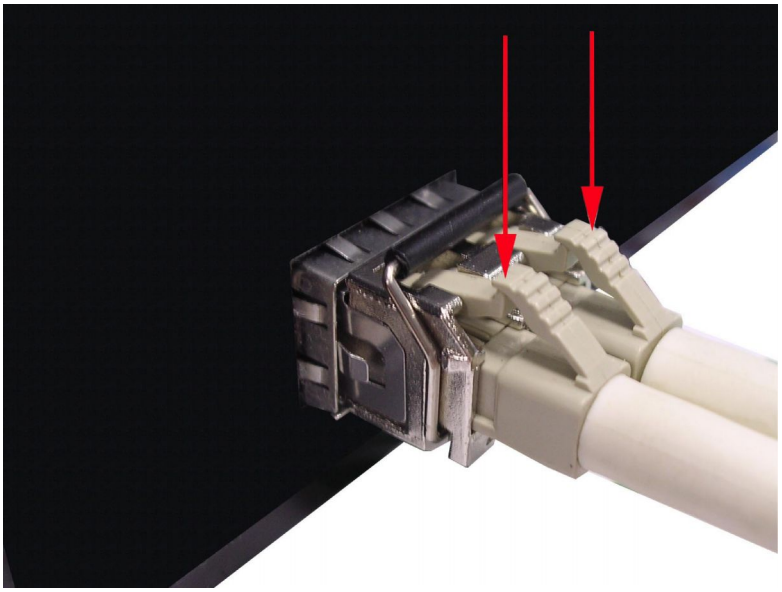
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

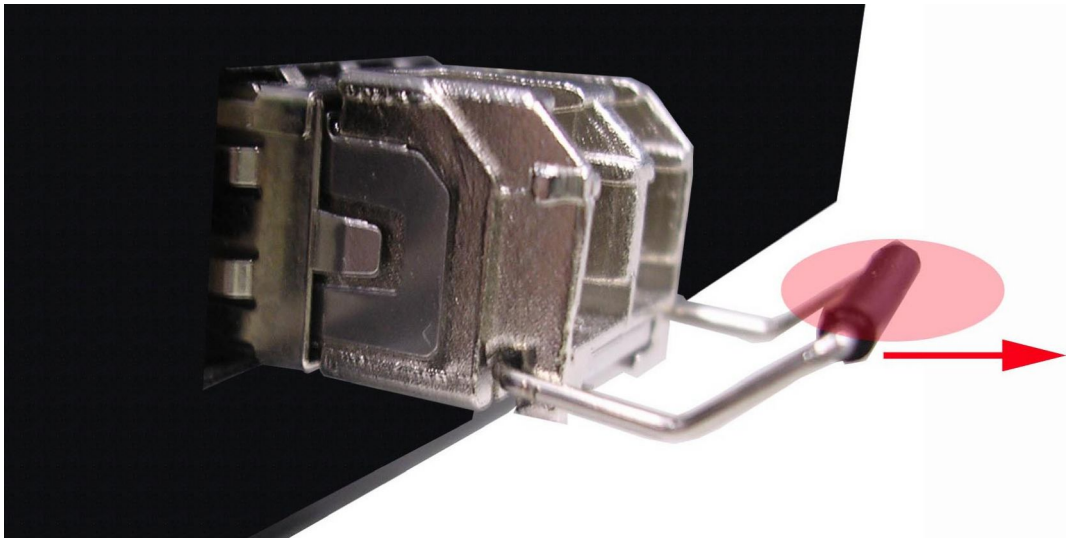
To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.



Remove LC connector

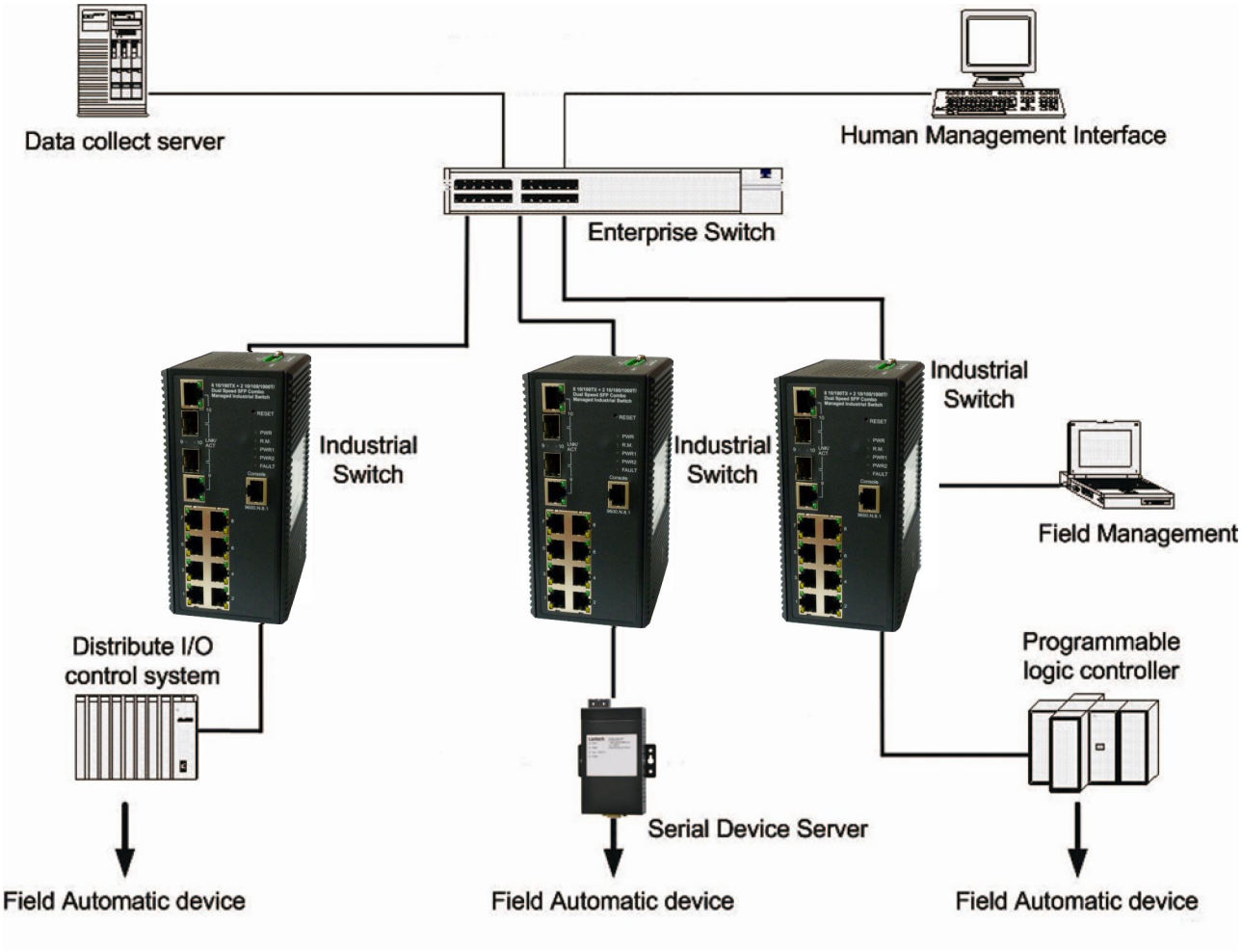
Second, push down the metal loop and pull the transceiver out by the plastic handle.



Pull out from the transceiver

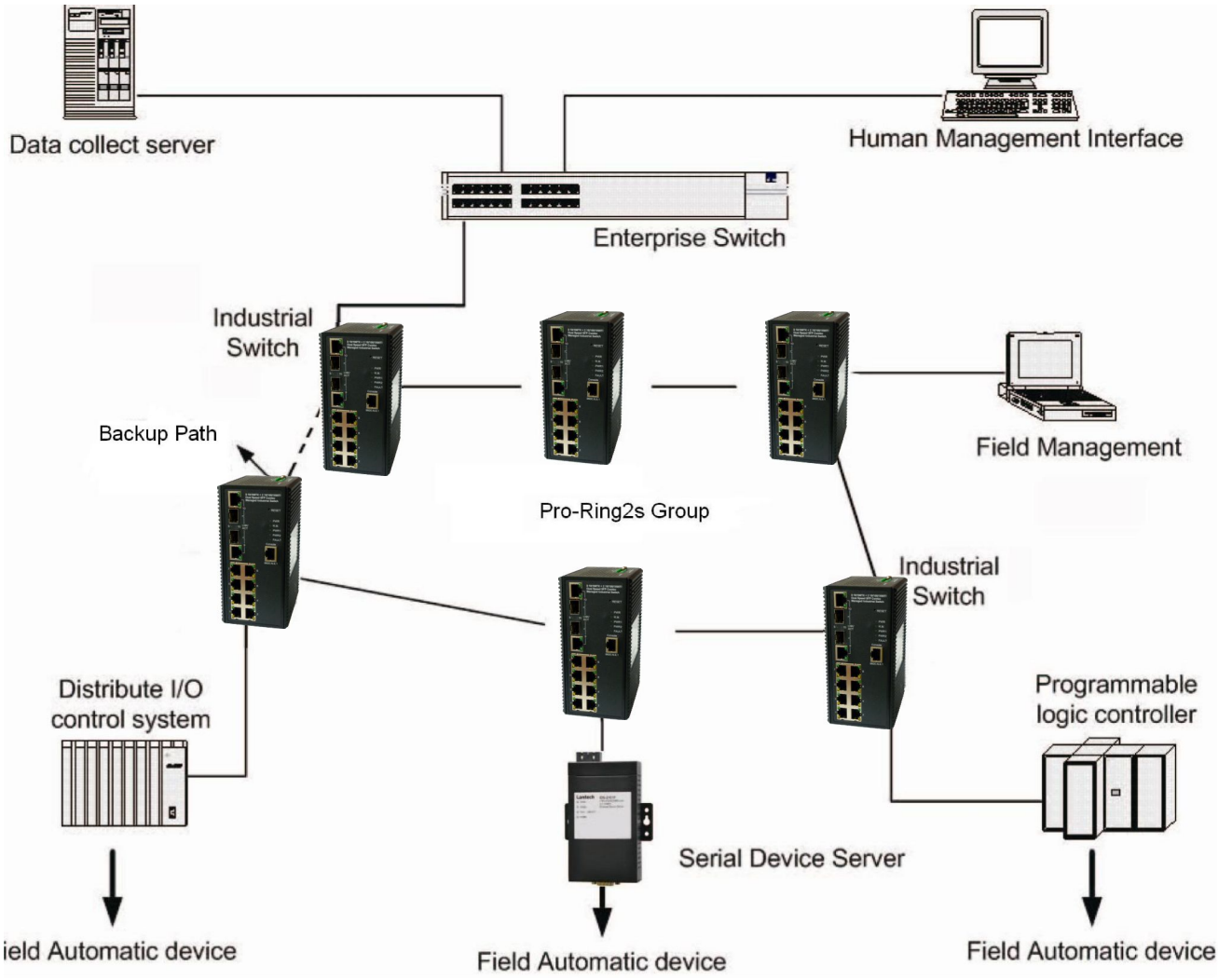
Chapter 4 Network Application

This chapter provides some sample applications to help user to have more actual idea of industrial switch function application. A sample application of the industrial switch is as below:



4.1 Pro-Ring2s Application

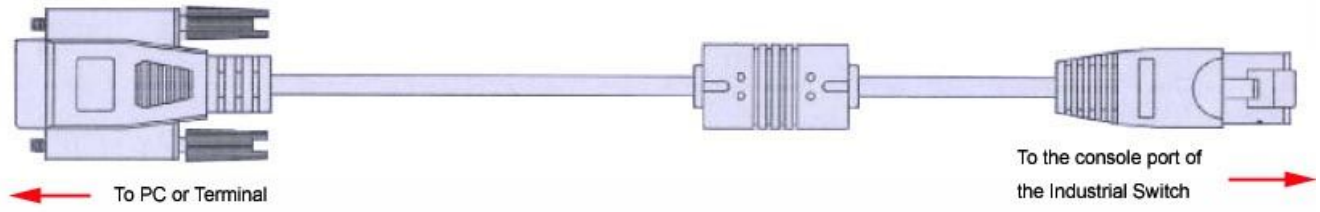
Pro-Ring II is a new Ring mechanism for Equitel Industrial Switches in which it eliminates the need to pre-set the Master switch in old Pro-Ring and yet to protect the network by much secure topologies than ever. Pro-Ring II works as a Ring Chain to reduce the risk of master switch linking down whereas the setup becomes much easier. Pro-Ring II can be backward compatible with old Pro-Ring by down-grading the Ring scheme to old one.

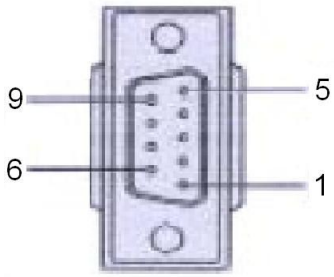


Chapter 5 Console Management

5.1 Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45 connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

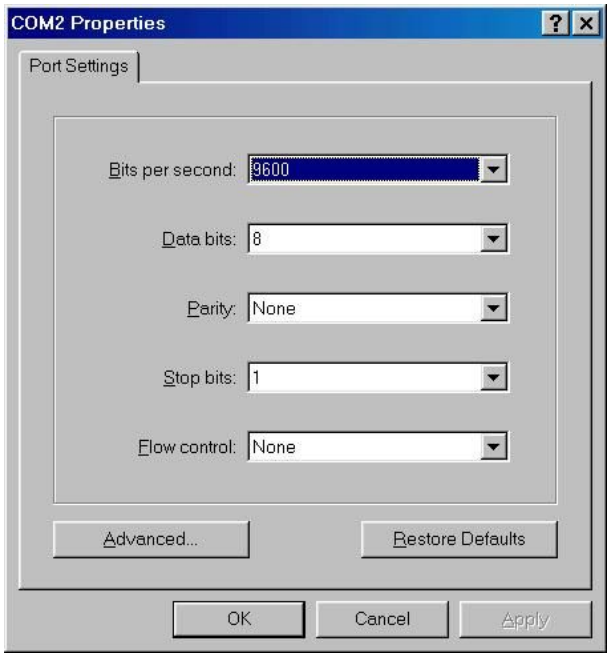
5.2 Pin Assignment

DB9 Connector	RJ-45 Connector	
NC	1	Orange/White
2	2	Orange
3	3	Green/White
NC	4	Blue
5	5	Blue/White
NC	6	Green
NC	7	Brown/White
NC	8	Brown

5.3 Login in the Console Interface

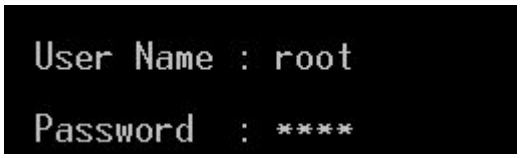
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to have the login prompt appears. Key in '**root**' (default value) for both User name and Password (use **Enter** key to switch), then press Enter and the Main Menu of console management appears. Please see below figure for login screen.



Console login interface

5.4 CLI Management

The system supports the console management—CLI command. After you log in on to the system, you will see a command prompt. To enter CLI management interface, type in “**enable**” command.

CLI command interface

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

6.1 About Web-based Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

6.2 Preparing for Web Management

Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **root**

6.3 System Login

1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**root**’.
5. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears.

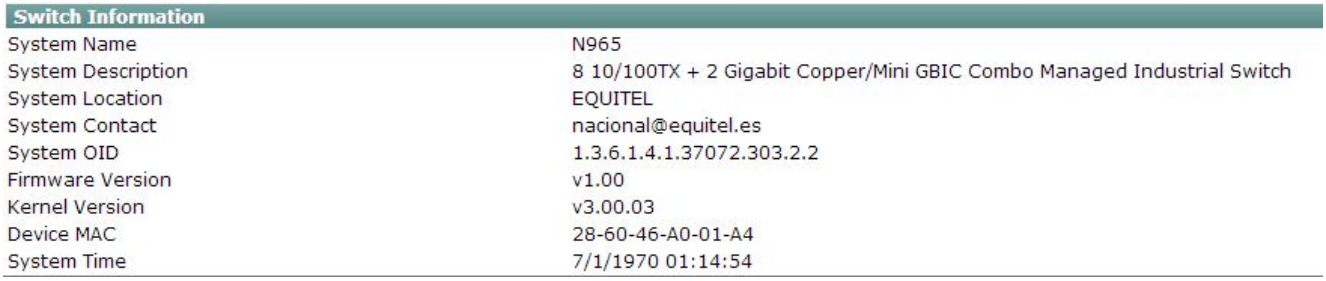
Login screen

6.4 System

6.4.1 General – Switch Information

User can find the system name, description, location and contact personnel to identify the switch. The version table below is a read-only field to show the basic information of the switch.

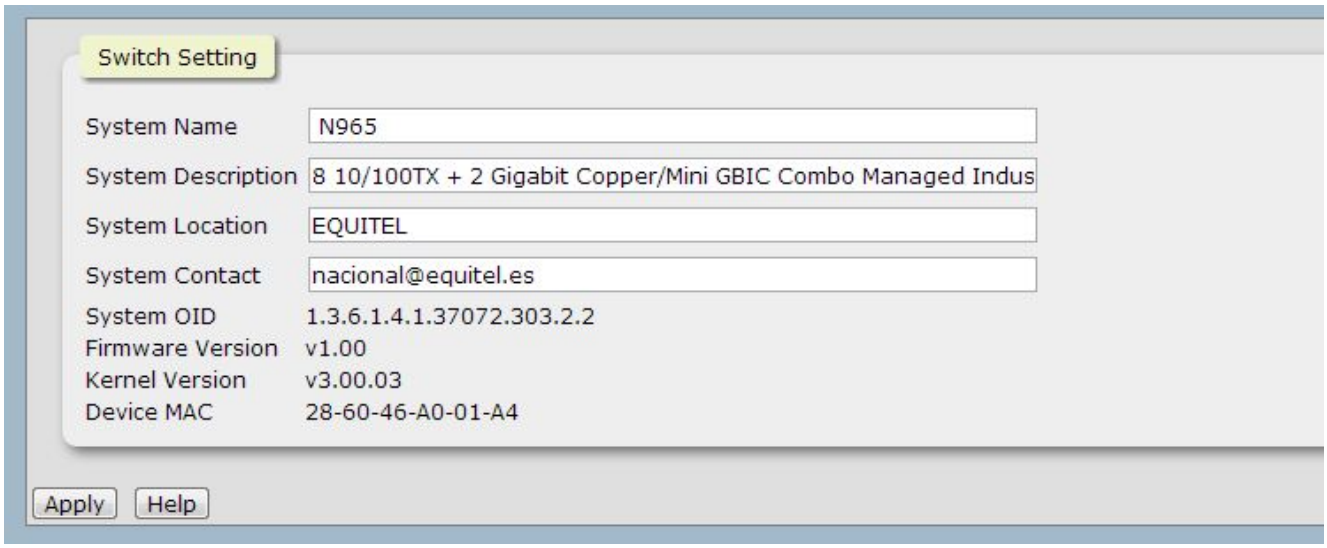
- **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)
- **System Description:** Describes the switch.
- **System Location:** Assign the switch physical location (The maximum length is 64 bytes).
- **System Contact:** Enter the name of contact person or organization.
- **System OID:** SNMP OID of switch
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer



Switch Information	
System Name	N965
System Description	8 10/100TX + 2 Gigabit Copper/Mini GBIC Combo Managed Industrial Switch
System Location	EQUITEL
System Contact	nacional@equitel.es
System OID	1.3.6.1.4.1.37072.303.2.2
Firmware Version	v1.00
Kernel Version	v3.00.03
Device MAC	28-60-46-A0-01-A4
System Time	7/1/1970 01:14:54

6.4.2 General – Asset

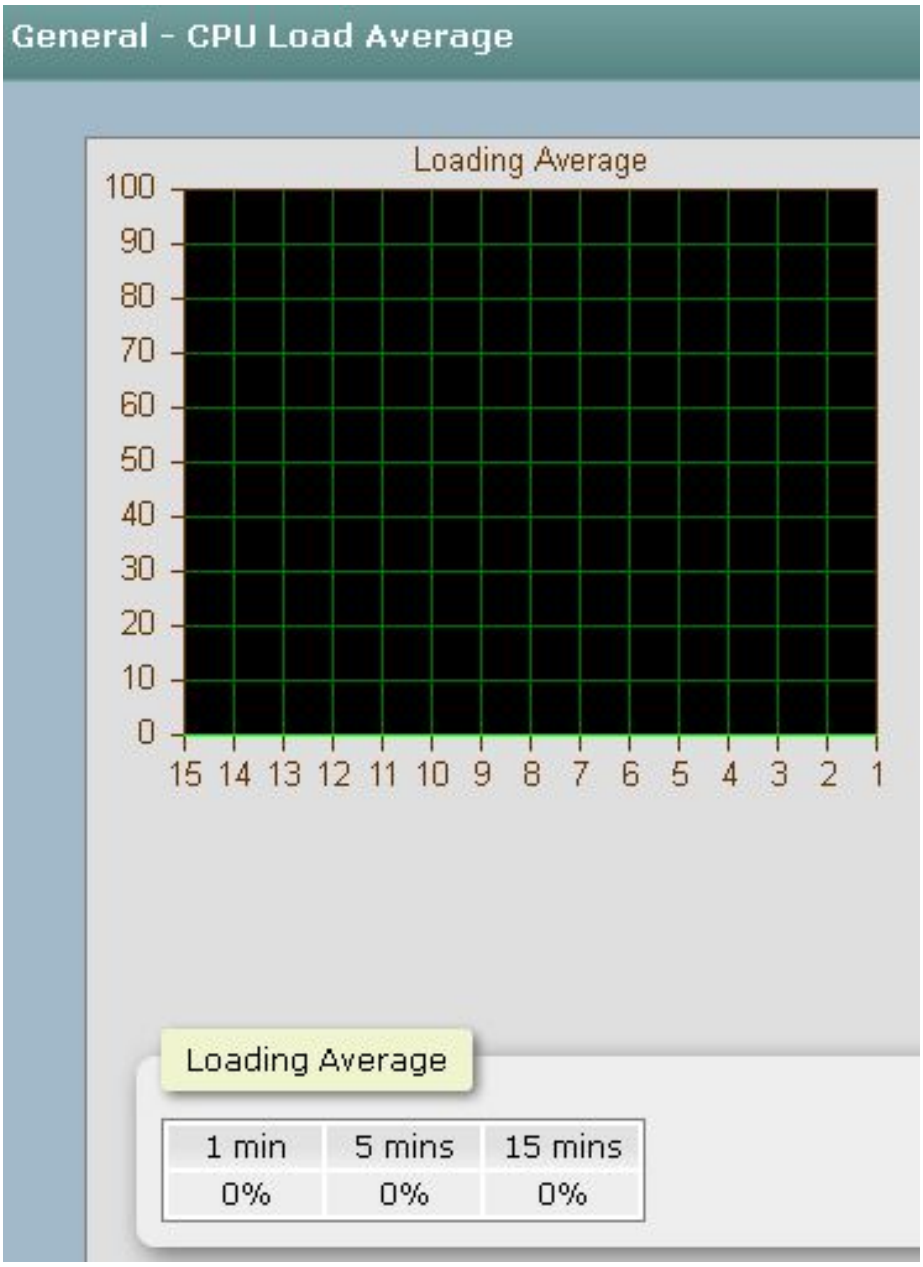
You can modify these information about System name 、System Description、System Location and System Contact in here.



Switch settings interface

6.4.2 General – CPU Load Average

Sometimes the user was worry about that ‘ Could my switch process too many network packets ? So the network throughput was keeping decreasing “. In this option, you can monitor the CPU of switch to see if the switch was in full loading status or not.


General - CPU Load Average
Loading Average
100
90
80
70
60
50
40
30
20
10
0
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
Loading Average
1 min
5 mins
15 mins
0%
0%
0%

6.5 Time - SNTP

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers to some time reference. Because time usually just advances, the time on different node stations will be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

Daylight saving time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server.
- **UTC Timezone:** Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

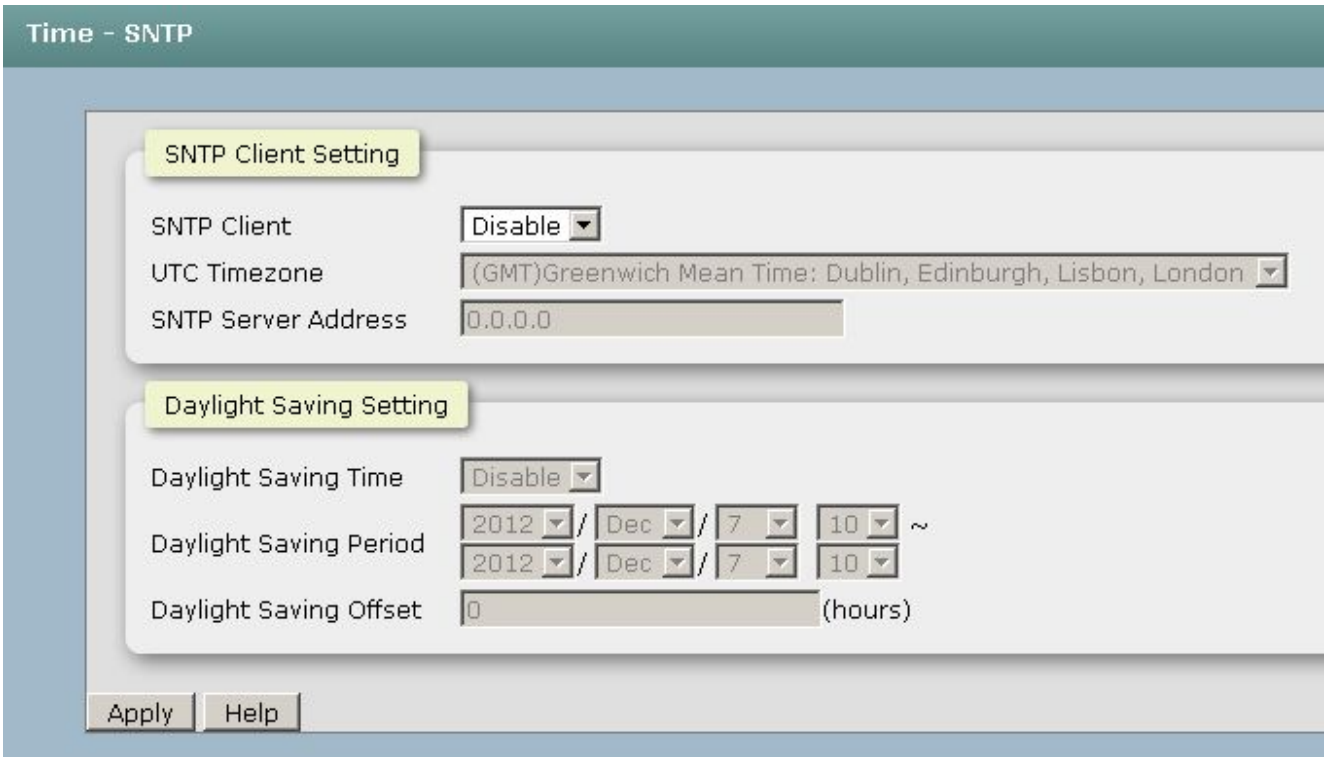
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard	-7 hours	5 am

PDT - Pacific Daylight		
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian	+10 hours	10 pm

Standard GST Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever Address:** Set the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **Daylight Saving Time:** This is used as a control switch to enable/disable daylight saving period and daylight saving offset. Users can configure Daylight Saving Period and Daylight Saving Offset in a certain period time and offset time while there is no need to enable daylight saving function. Afterwards, users can just set this item as enable without assign Daylight Saving Period and Daylight Saving Offset again.
- **Daylight Saving Period:** Set up the Daylight Saving beginning date/time and Daylight Saving ending date/time. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

  For example, key in '20070701 02:00' and '20071104 02:04' in the two column fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- **Daylight Saving Offset :** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.
- Click Apply to have the configuration take effect.



SNTP Configuration interface

6.6 Account - Admin

Change web management login user name and password for the management security issue.

- **User name:** Type in the new user name (The default is ‘root’)
- **New Password:** Type in the new password (The default is ‘root’)
- **Confirm password:** Re-type the new password
- And then, click Apply

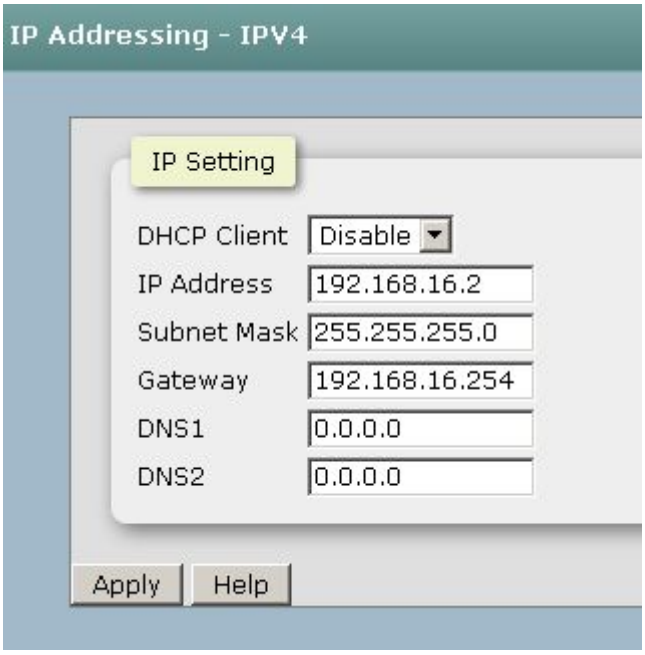
Account Authentication interface

6.7 IP Addressing – IPV4

The switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the switch.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks **Apply**, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
- **Gateway:** Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.16.254.

- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click Apply.



IP Addressing interface

6.8 Syslog

This page allows the user to decide whether to send the system event log, and select the mode which the system event log will be sent to client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab. There are four types of event—Device Cold Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the event log.

Syslog Configuration

Syslog Configuration interface

- **Syslog Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**. 'Client Only' means the system event log will only be sent to this interface of the switch, but on the other hand 'Server Only' means the system log will only be sent to the remote system log server with its IP assigned. If the mode is set in 'Both', the system event log will be sent to the remote server and this interface.
- **SysLog Server IP Address:** When the 'Syslog Mode' item is set as Server Only/Both, the user has to assign the system log server IP address to which the log will be sent.
- Make sure the selected mode is correct, and click Apply to have the setting take effect.

6.9 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

SNMP - Agent

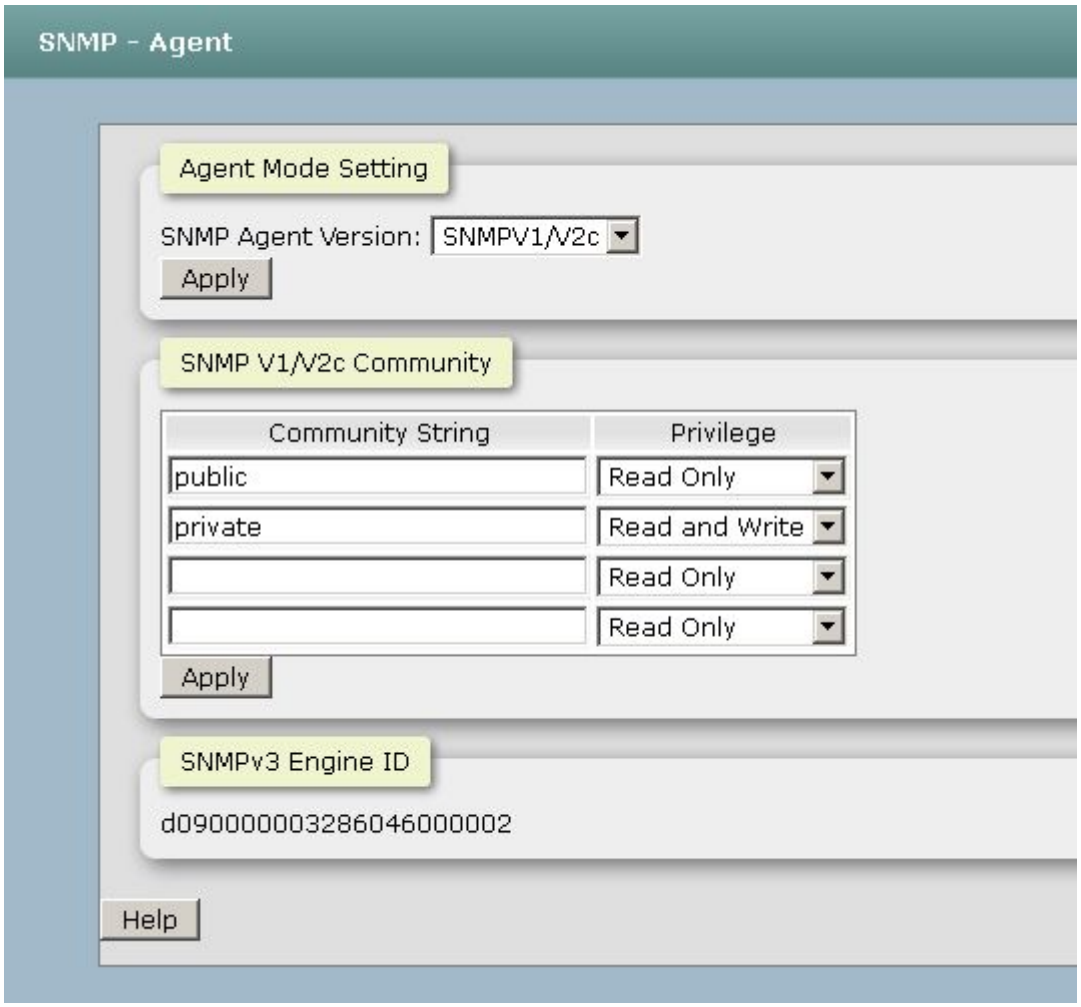
- **Agent Mode:** Select the SNMP version(V1/V2c or V3) that you want to use it. And then click Change to switch to the selected SNMP version mode.

- **SNMP V1V2c Community**

Here you can define the new community string set and remove the unwanted community string.

- **Community String:** Fill the name string.
- **Privilege:** Read only. Enables requests accompanied by this community string to display MIB-object information.

  Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click. Apply

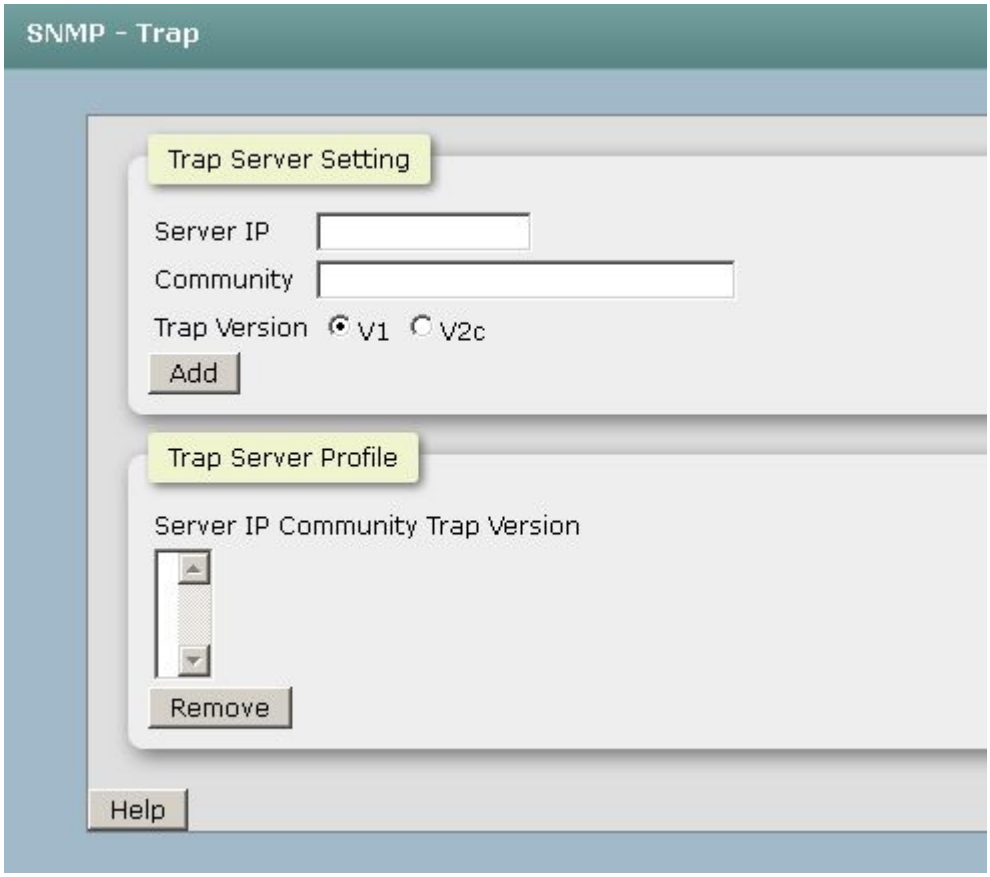


SNMP Agent Configuration interface

6.20.1 SNMP Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **Server IP :** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Click Add.
- To remove the community string, select the community string listed in the current managers field and click Remove.

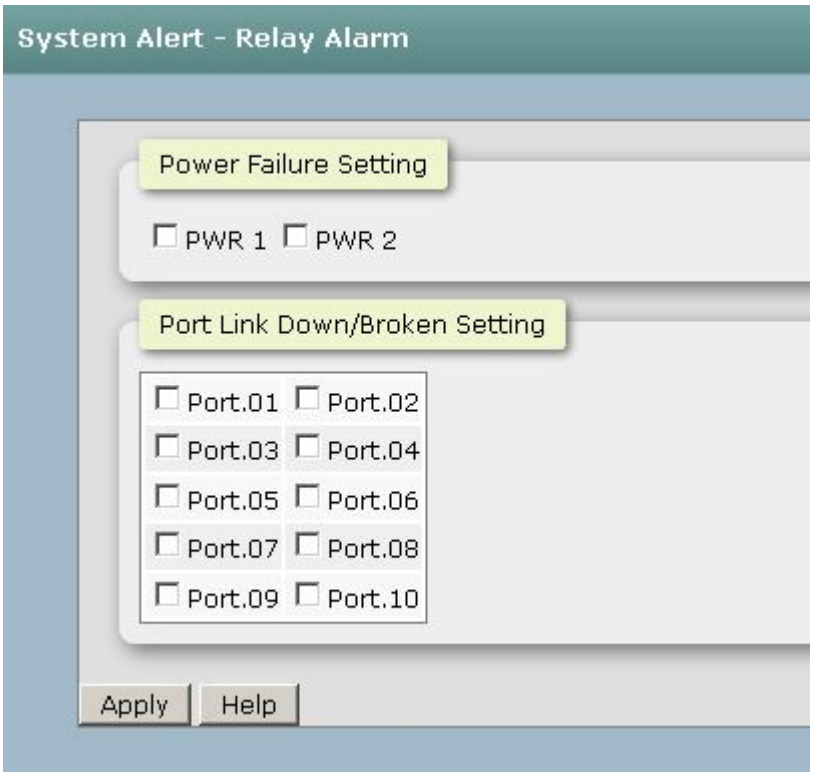


Trap Managers interface

6.10 System Alert - Relay Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of '**Wiring the Fault Alarm Contact**' for the failure detection.

- **Power Failure Setting:** Tick the check box to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken Setting:** Tick the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.



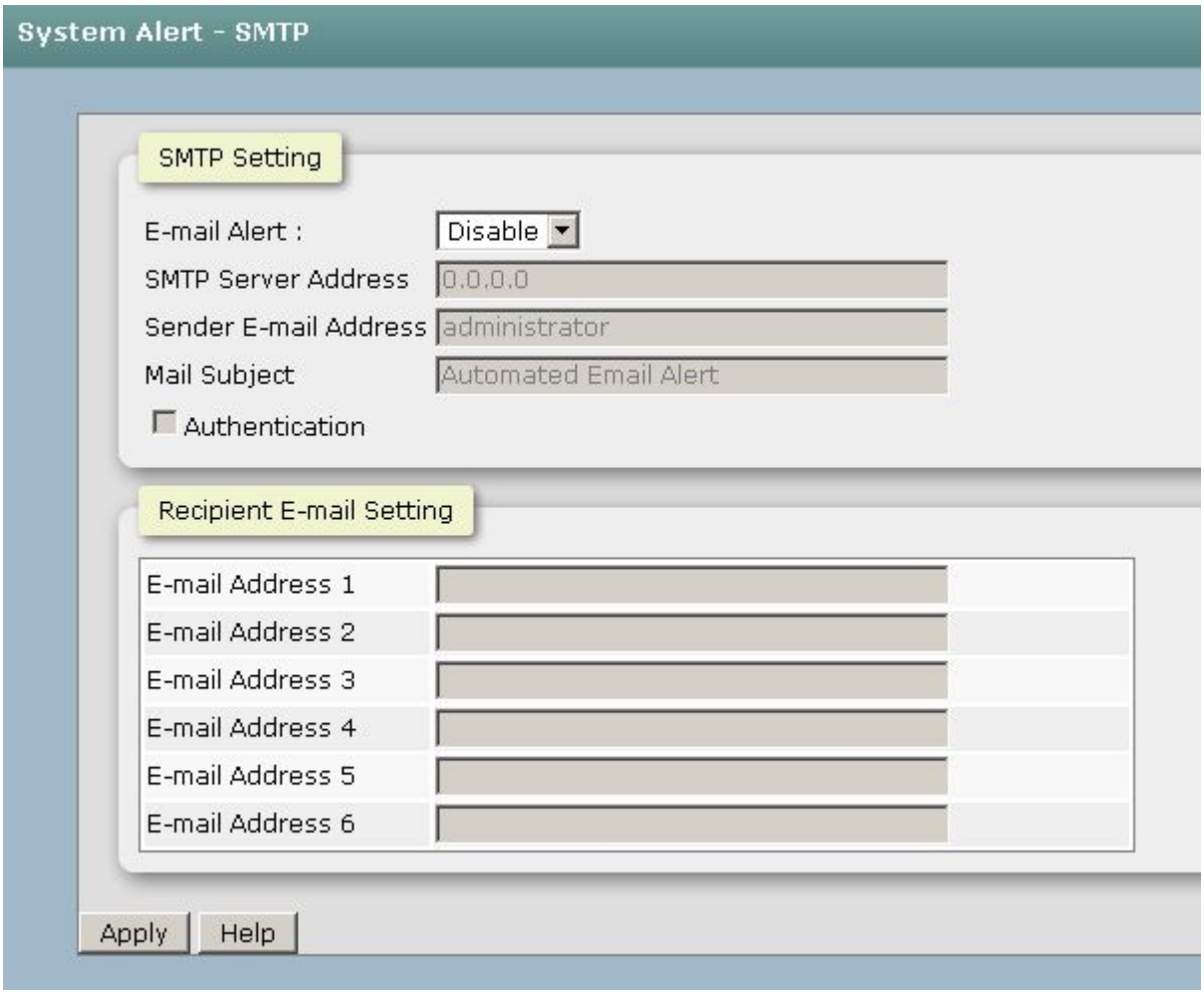
Fault Relay Alarm interface

6.8.1 System Alert - SMTP

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP, mail subject, sender, mail account, password, and the recipient email addresses which the e-mail alert will send to. There

are also five types of event—Device Cold Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the e-mail alert. Besides, this function provides the authentication mechanism including an authentication step through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert:** With this function being enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP:** Assign the mail server IP address (when **Email Alert** is enabled, this function will then be available).
- **Sender Email Address:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the e-mail alert comes from.
- **Mail Subject:** Input the subject of Email.
- **Authentication:** Having ticked this checkbox, the mail account, password and confirm password column fields will then show up. Configure the email account and password for authentication when this switch logs in to the SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password for the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also fill each of the column fields with up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



6.8.2 System Alert - Event

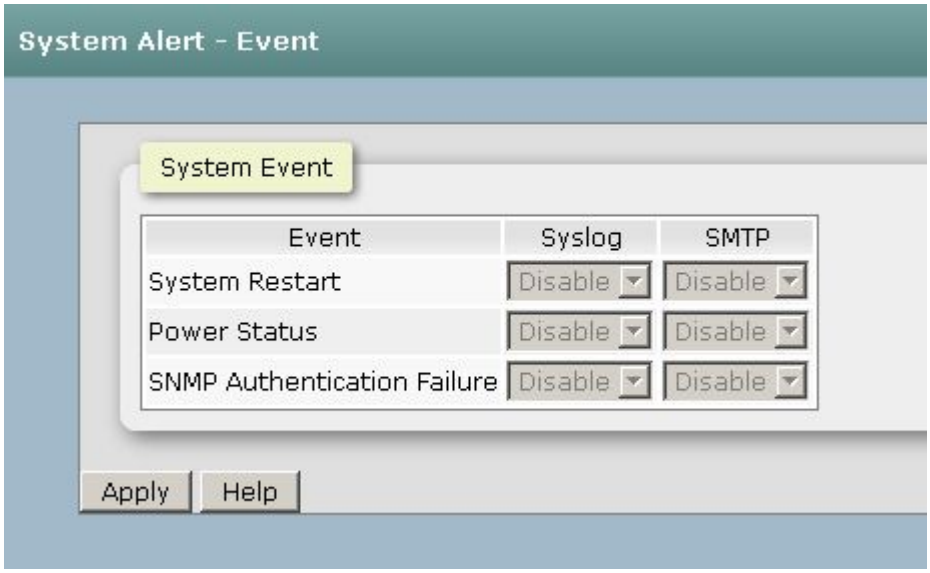
Having ticked the **Syslog**/**SMTP** checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

- **System event selection:** There are 3 event types—Device Cold Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.
  - **System Restart:** When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **Power Status:** When the power consumption about PoE was unstable, he

system will issue the event log/email alert to the system log/SMTP server respectively.

- **SNMP Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.

.



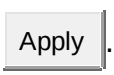
Event Configuration interface

6.11 DHCP Server

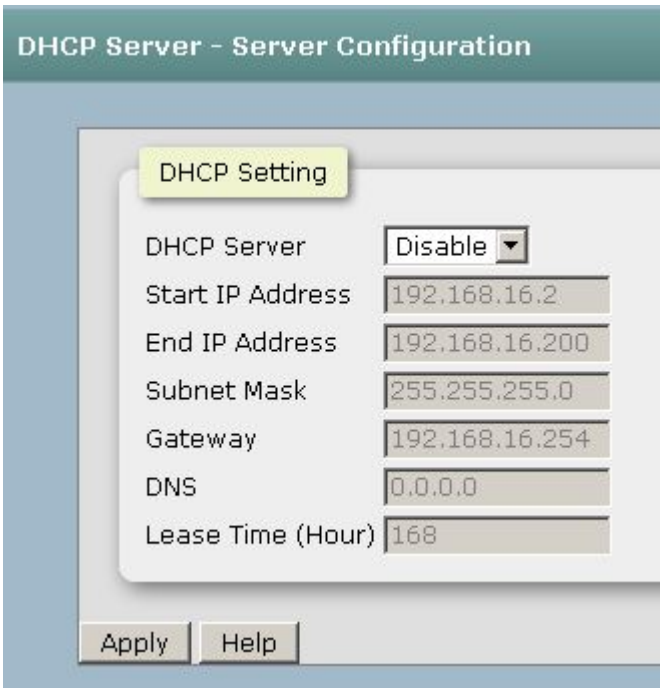
DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

6.6.1 DHCP Server - Server configuration

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **Start IP Address:** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.16.100 ~ 192.168.16.200. In contrast, 192.168.16.100 is the Low IP address.
- **End IP Address:** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.16.100 ~ 192.168.16.200. In contrast, 192.168.16.200 is the High IP address.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time (Hour):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click 

.

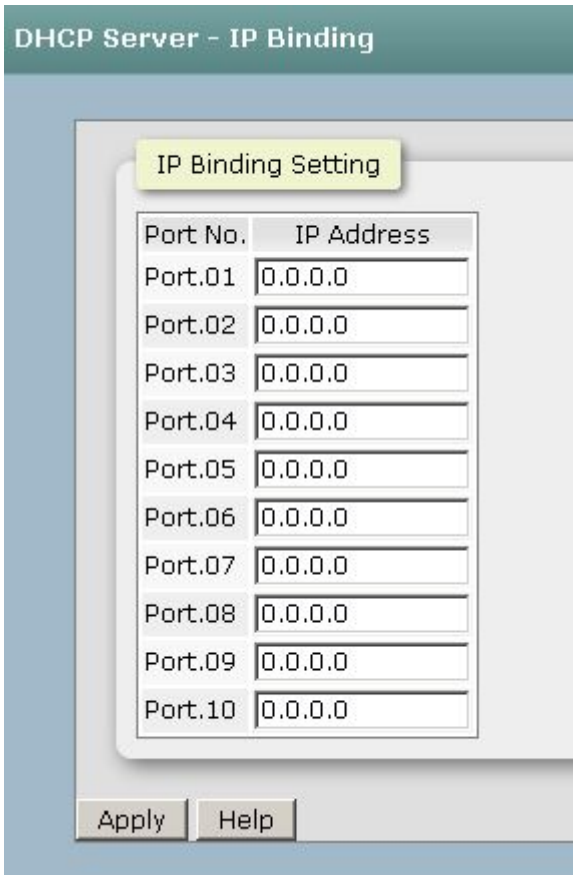


6.6.2 Client Table

When the DHCP server function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, status and lease time.

6.6.3 IP Bindings

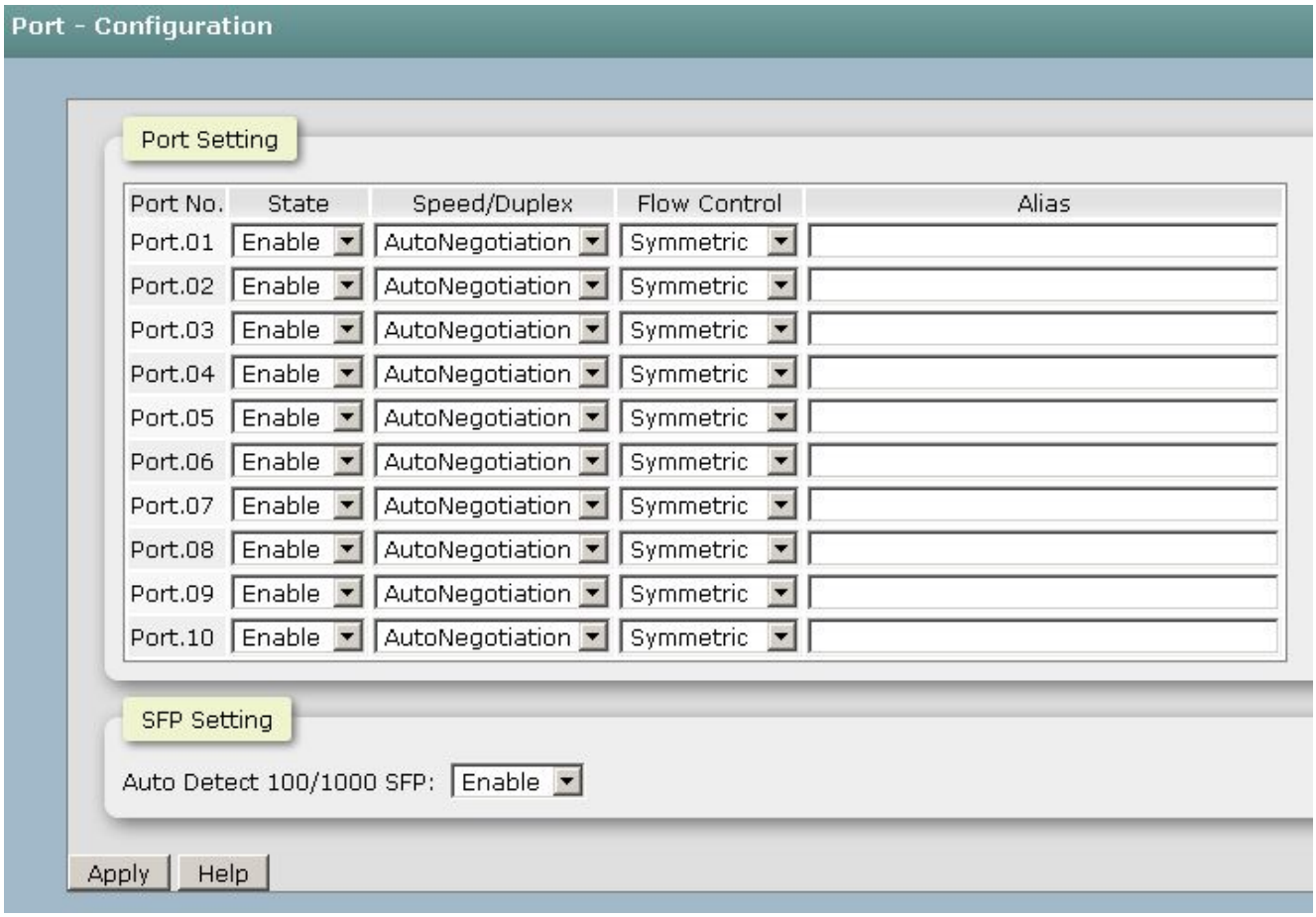
Assign the dynamic IP address bound with the port to the connected client. The user is allowed to fill each port column with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port.


DHCP Server - IP Binding
IP Binding Setting
Port No.
IP Address
Port.01 0.0.0.0
Port.02 0.0.0.0
Port.03 0.0.0.0
Port.04 0.0.0.0
Port.05 0.0.0.0
Port.06 0.0.0.0
Port.07 0.0.0.0
Port.08 0.0.0.0
Port.09 0.0.0.0
Port.10 0.0.0.0
Apply
Help

6.12 Port - Configuration

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

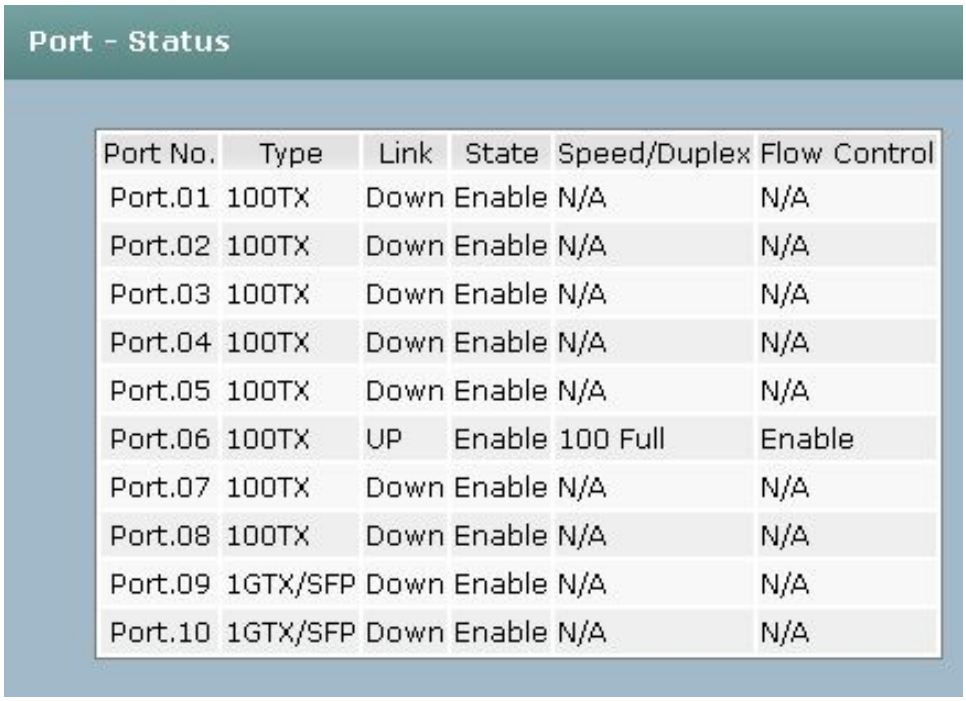
- **Port No.:** The port number which you want to be configured.
- **State:** Current port state. The port can be set to disable or enable mode. If the port state is set as ‘Disable’, it will not receive or transmit any packet..
- **Speed/Diplex:** It can be set as auto or set speed and negotiated way manually.
- **Flow Control:** Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
- **Alies:** Add description of each port to let the manager know the connected device of each port, it will be showed by NMS utility.
- Click Apply to have the configuration take effect.



Port Control interface

6.13 Port Status

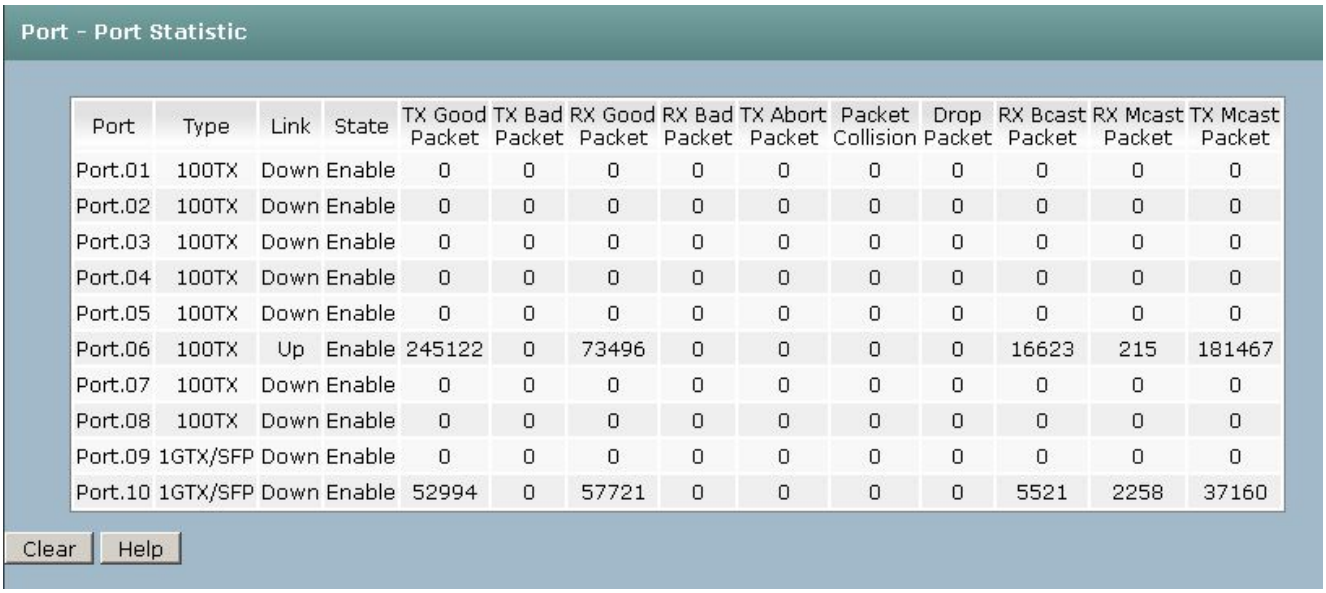
It will show you the status of port configuration setting .


Port - Status
Port No. Type Link State Speed/Duplex Flow Control
Port.01 100TX Down Enable N/A N/A
Port.02 100TX Down Enable N/A N/A
Port.03 100TX Down Enable N/A N/A
Port.04 100TX Down Enable N/A N/A
Port.05 100TX Down Enable N/A N/A
Port.06 100TX UP Enable 100 Full Enable
Port.07 100TX Down Enable N/A N/A
Port.08 100TX Down Enable N/A N/A
Port.09 1GTX/SFP Down Enable N/A N/A
Port.10 1GTX/SFP Down Enable N/A N/A

6.14 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click Clear button to clean all counts.


Port - Port Statistic
Port Type Link State TX Good Packet TX Bad Packet RX Good Packet RX Bad Packet TX Abort Packet Packet Collision Drop Packet RX Bcast Packet RX Mcast Packet TX Mcast Packet
Port.01 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.02 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.03 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.04 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.05 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.06 100TX Up Enable 245122 0 73496 0 0 0 0 16623 215 181467
Port.07 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.08 100TX Down Enable 0 0 0 0 0 0 0 0 0 0
Port.09 1GTX/SFP Down Enable 0 0 0 0 0 0 0 0 0 0
Port.10 1GTX/SFP Down Enable 52994 0 57721 0 0 0 0 5521 2258 37160
Clear
Help

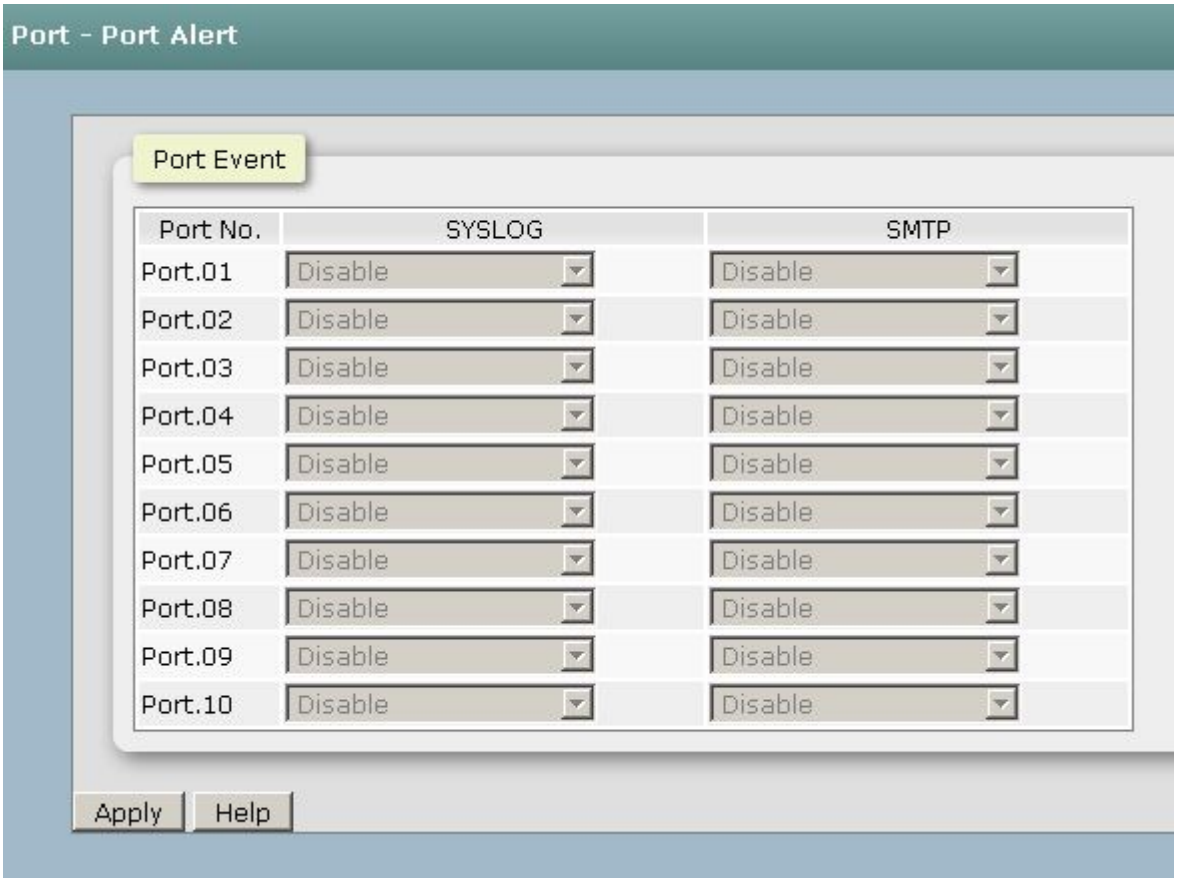
Port Statistics interfac

6.15 Port – Port Alert

Having ticked the **Syslog**/**SMTP** checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

- **System event selection:** There are 3 event types—Device Cold Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.
  - **Device cold start:** When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **MAC Violation:** When the MAC address has violated, the system will issue the event log/email alert to the system log/SMTP server respectively.

- **Port event selection:** Also, before the drop-down menu items are available, the **Syslog Client Mode** selection item on the Syslog Configuration tab and the **E-mail Alert** selection item on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—**Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will only issue a log message when the link-up event of the port occurs.
  - **Link Down:** The system will only issue a log message when the link-down event of port occurs.
  - **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.

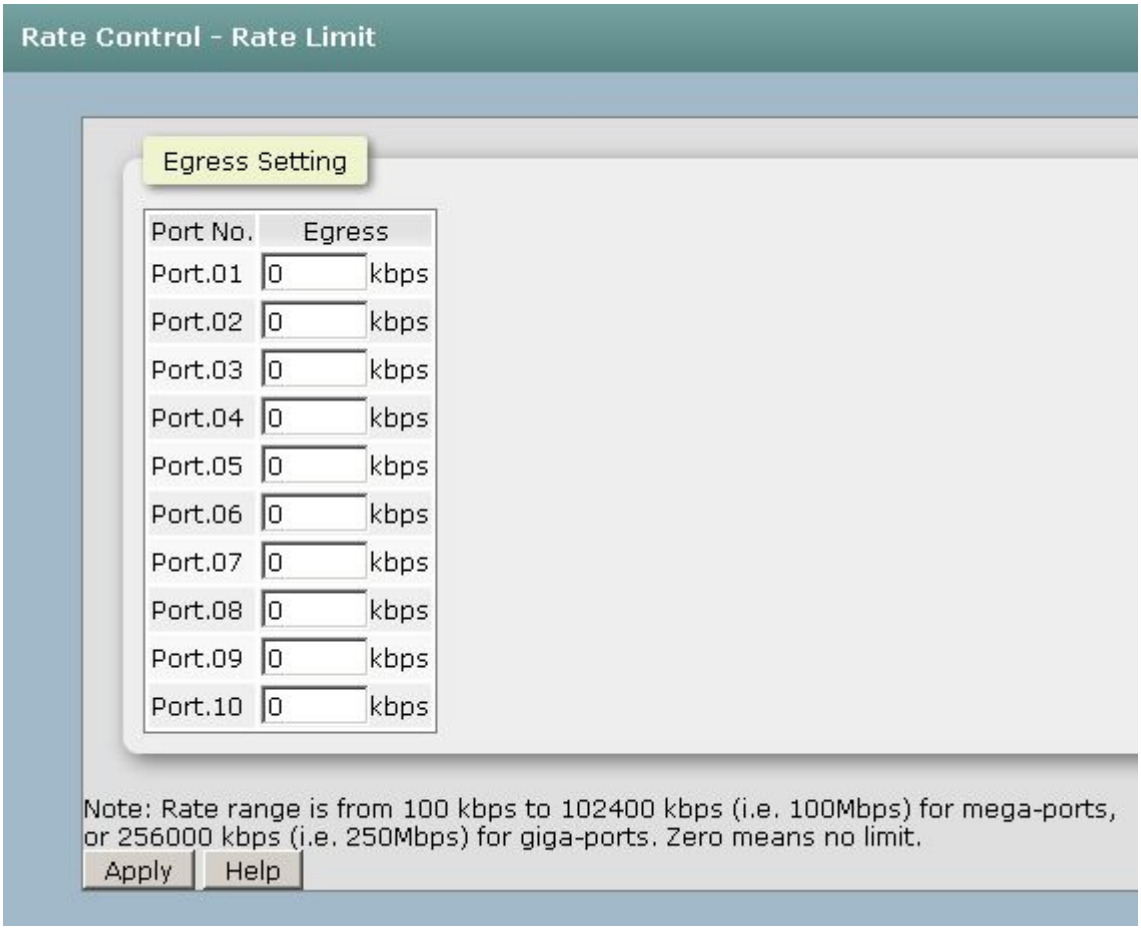


6.16 Rate Control –Rate Limit

You can set up every port's bandwidth rate and frame limitation type.

All the ports support port egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate

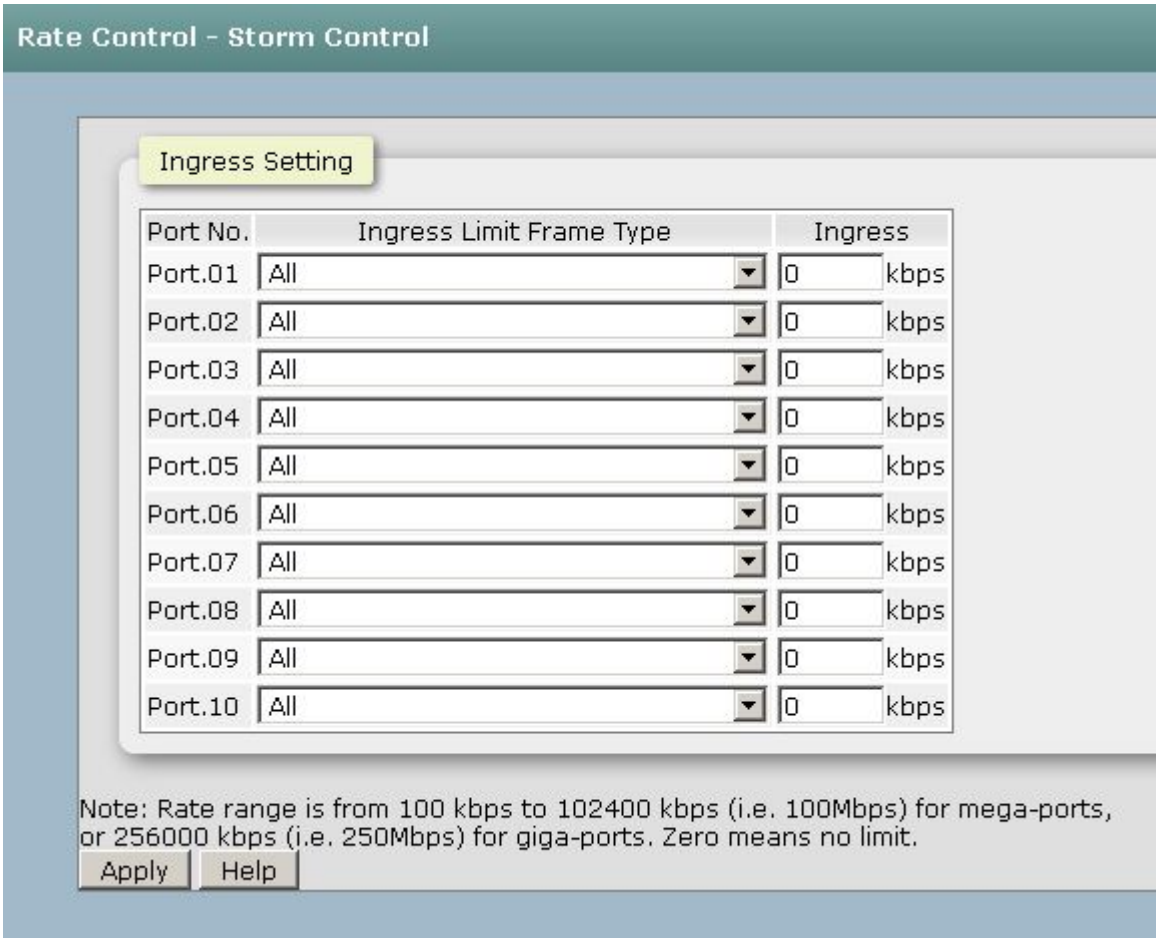
- And then, click Apply to apply the settings



- **Storm Control:** select the frame type that wants to filter. There are four frame types for selecting:
  - **All**
  - **Broadcast/Multicast/Flooded Unicast**
  - **Broadcast/Multicast**
  - **Broadcast only**

  Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Bbroadcast only** types are only for ingress frames. The egress rate only supports **All** type.

- And then, click Apply to apply the settings

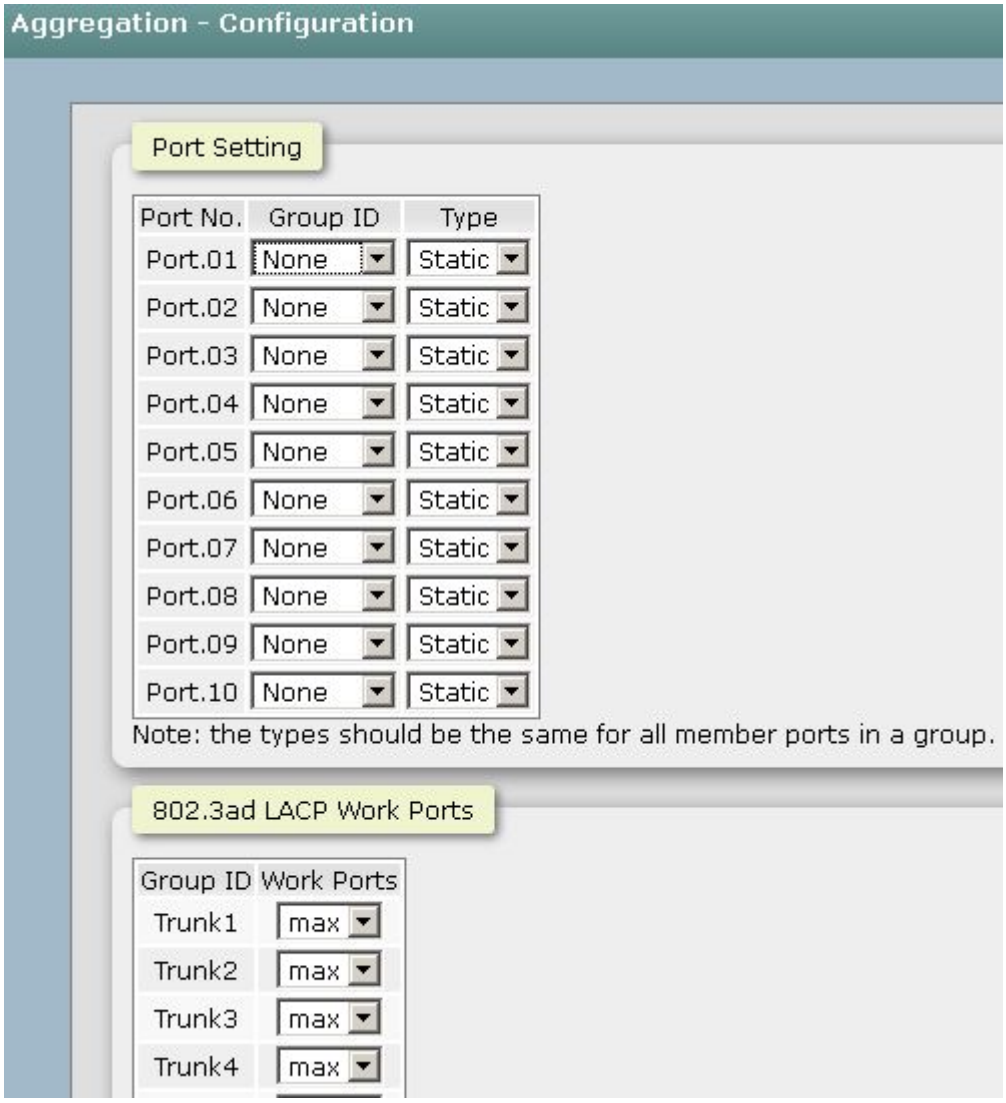

Rate Control - Storm Control
Ingress Setting
Port No.
Ingress Limit Frame Type
Ingress
Port.01 All 0 kbps
Port.02 All 0 kbps
Port.03 All 0 kbps
Port.04 All 0 kbps
Port.05 All 0 kbps
Port.06 All 0 kbps
Port.07 All 0 kbps
Port.08 All 0 kbps
Port.09 All 0 kbps
Port.10 All 0 kbps
Note: Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.
Apply
Help

6.17 Aggregation - Configuration

Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

6.17.1 Configuration

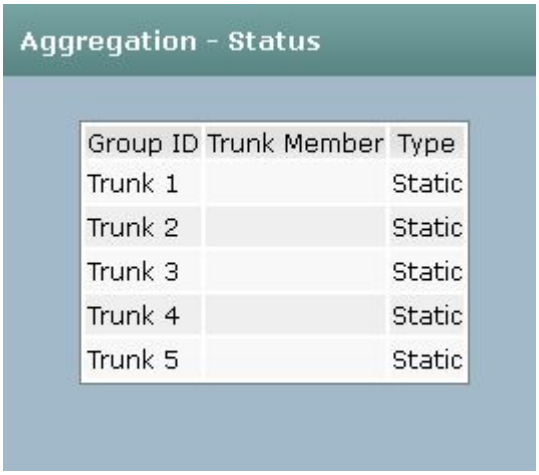
- **Group ID:** There are 5 trunk groups to be selected. Assign the "**Group ID**" to the trunk group.
- **TYPE:** When choose LACP, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work ports:** This column field allows the user to choose the total number of active port up to four. With **LACP static trunk group**, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a **static trunk group** (non-LACP), the number of work ports must equal the total number of group member ports.
- Click Apply.



Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

6.17.2 Aggregator – Status

You can check the setting of Port aggregation in Status.



6.18 Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

6.18.1 RSTP Setting

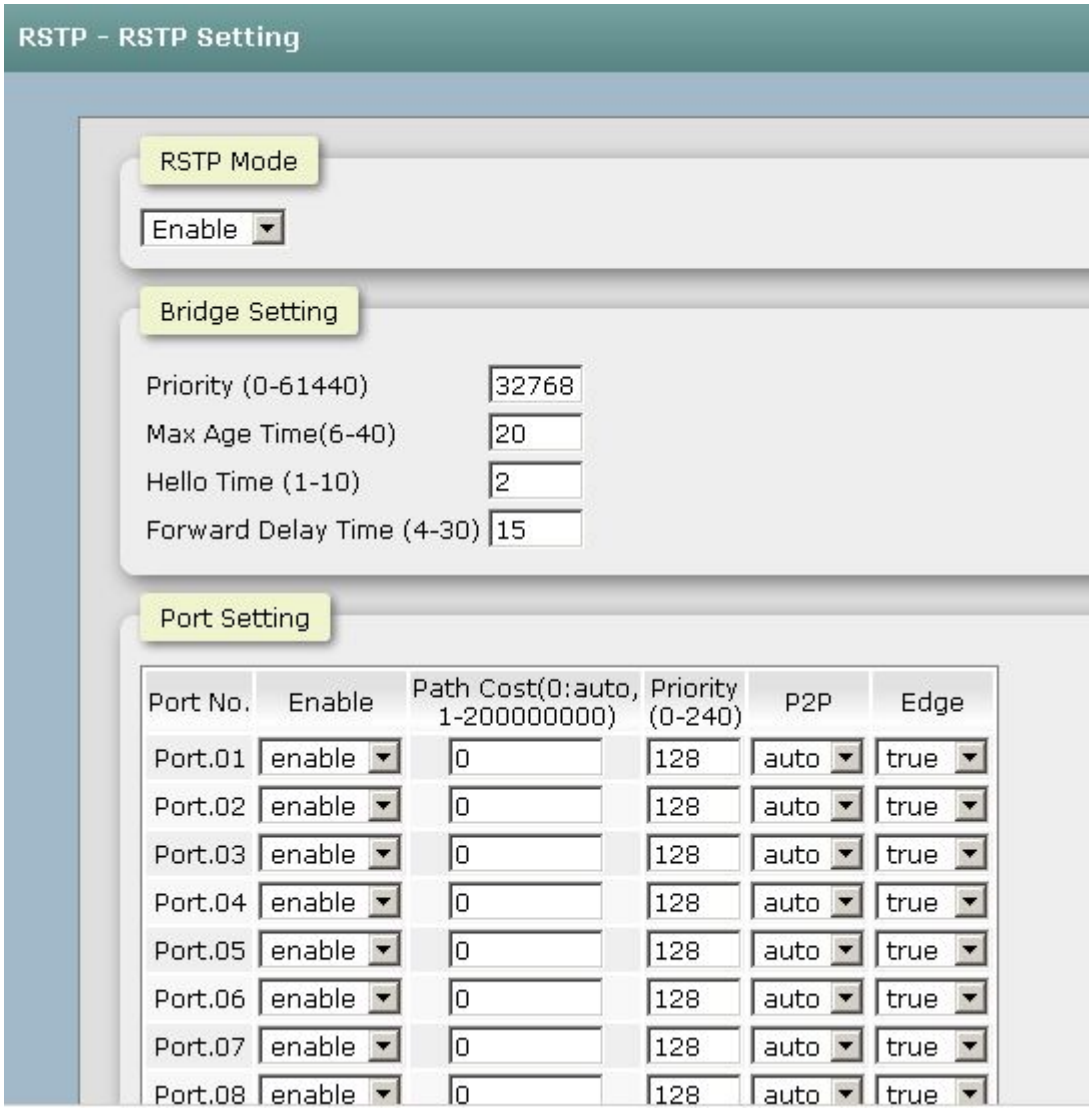
This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

- **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
- **Priority :** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
- **Max Age :** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time :** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time :** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

- **Enable:** Select the port which you want to be enabled with RSTP.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
- **P2P:** The rapid state transitions possible within RSTP are dependent upon whether

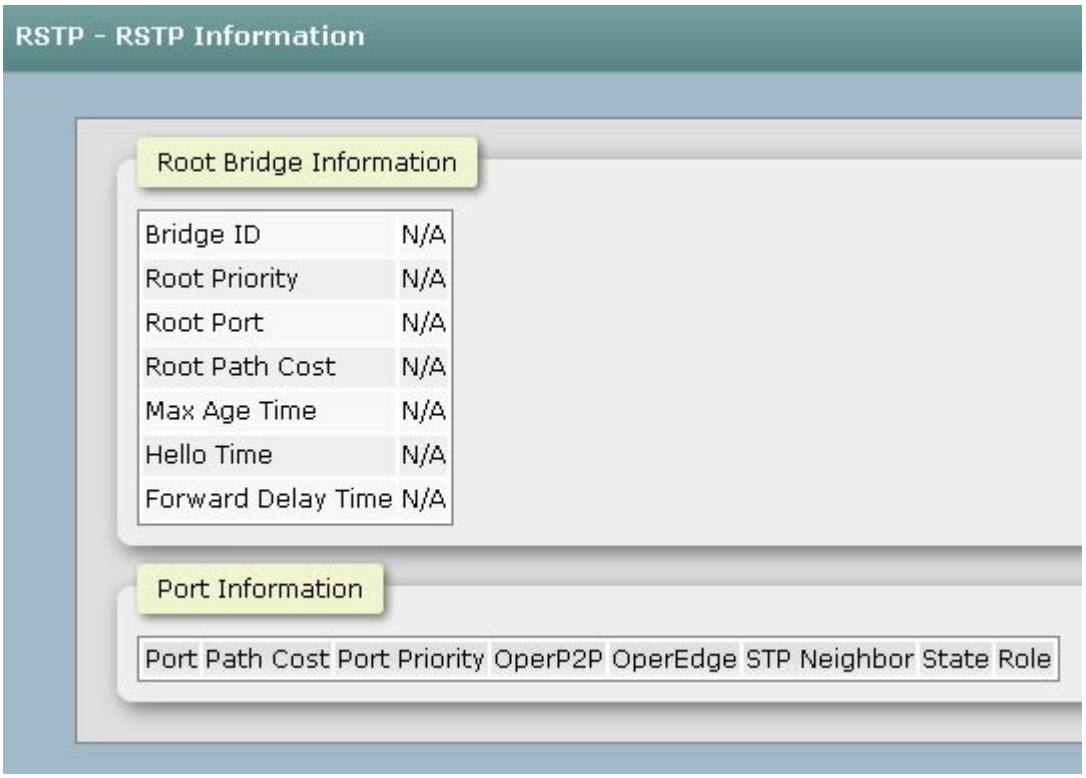
the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means the port is regarded as a point-to-point link. False means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers.

- **Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- Click Apply.


RSTP - RSTP Setting
RSTP Mode
Enable
Bridge Setting
Priority (0-61440) 32768
Max Age Time(6-40) 20
Hello Time (1-10) 2
Forward Delay Time (4-30) 15
Port Setting
Port No. Enable Path Cost(0:auto, 1-200000000) Priority (0-240) P2P Edge
Port.01 enable 0 128 auto true
Port.02 enable 0 128 auto true
Port.03 enable 0 128 auto true
Port.04 enable 0 128 auto true
Port.05 enable 0 128 auto true
Port.06 enable 0 128 auto true
Port.07 enable 0 128 auto true
Port.08 enable 0 128 auto true

6.18.2 RSTP Information

This web page provides the port and switch information about RSTP.

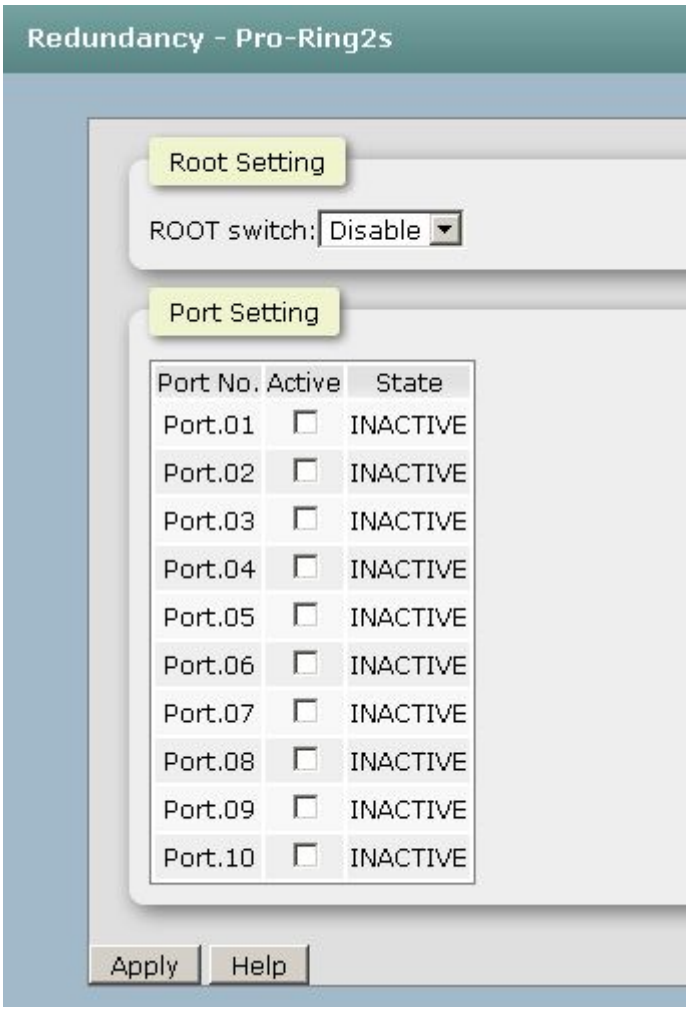

RSTP - RSTP Information
Root Bridge Information
Bridge ID N/A
Root Priority N/A
Root Port N/A
Root Path Cost N/A
Max Age Time N/A
Hello Time N/A
Forward Delay Time N/A
Port Information
Port Path Cost Port Priority OperP2P OperEdge STP Neighbor State Role

RSTP System Configuration interface

6.19 Pro-Ring II S

Pro-Ring IIs is a new Ring mechanism for Equitel Industrial Switches in which it protects the network by flexible topology than ever. Pro-Ring IIs works as a Single Ring and Multiple Ring to recover the broken ring in less than 20 ms for up to 50 switch nodes..

- **Root Switch:** To enable the X-Ring function, first you must set your switch as Enable or Backup, “Enable” means this switch will play the role of root switch, “Backup” means this switch will take over the role of root switch when the original root switch fail.
- **Port setting:** set the port which you want to build the Ring topology. usually set as G1 and G2. With some advance redundancy solution like Couple ring and Dual homing, if you are confused about which port was needed to enable, just select all the port which was responsible for uplink.
- And then, click Apply to have the configuration take effect.



RSTP Port Configuration interface

6.20 Multicast Support

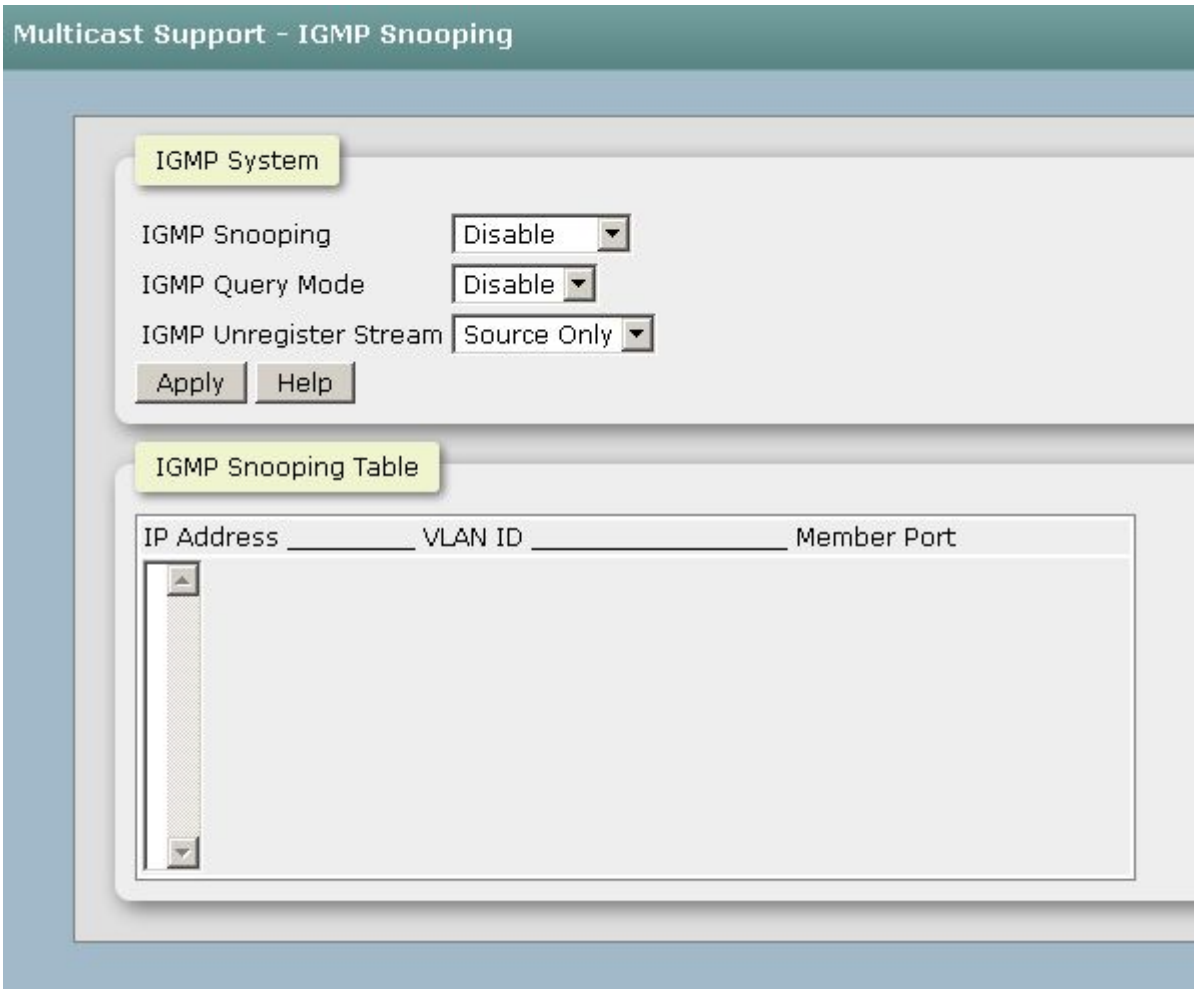
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch. IGMP have three fundamental types of message shown as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

6.20.1 IGMP Snooping

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then the IGMP snooping information displays. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.
- **IGMP Unregister Stream:** let the switch know how to process the Multicast data stream which was unregistered with IGMP Query.
- Click Apply.



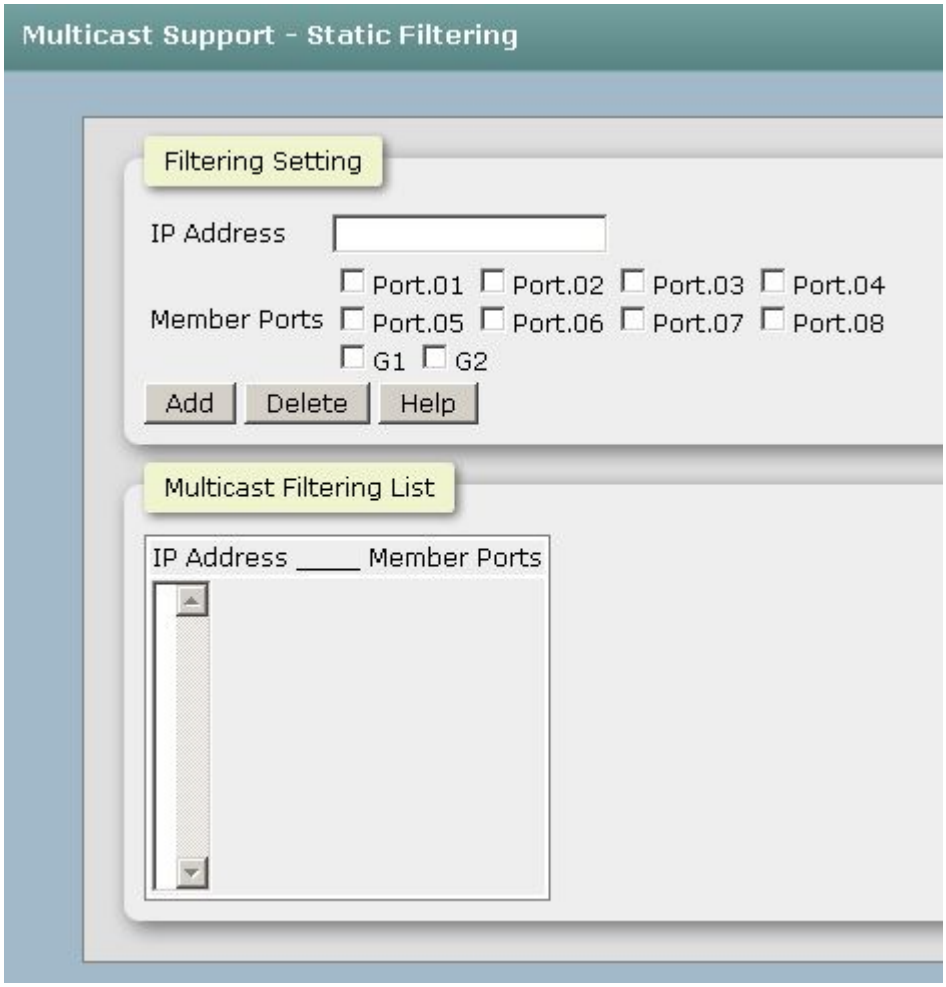
IGMP Configuration interface

6.20.2 Static Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.

- Click Add to append a new filter of multicast to the field, or select the filter in the field and click Delete to remove it.

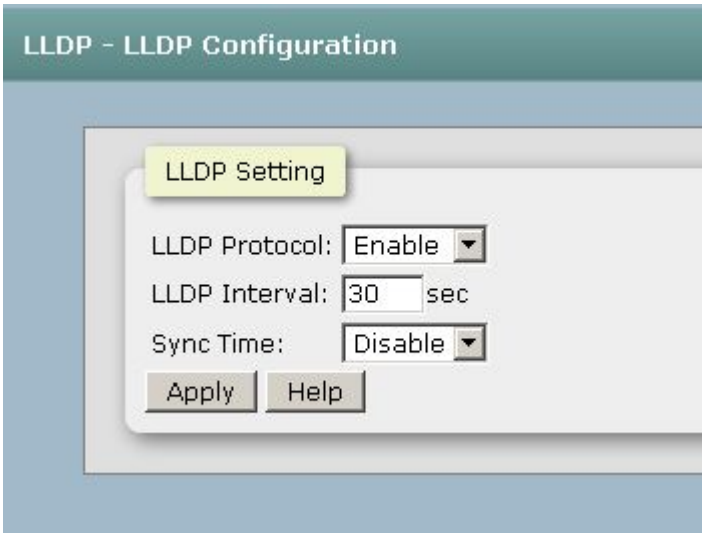


6.21 LLDP

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

6.21.1 LLDP Configuration

- **LLDP Protocol**: Pull down the selection menu to disable or enable LLDP function.
- **LLDP Interval**: Set the interval of advertising the switch's information to other nodes
- **Sync Time**: How long will the switch Sync the LLDP information..
- Click Apply.



LLDP Interface

6.22.1 LLDP Neighbors

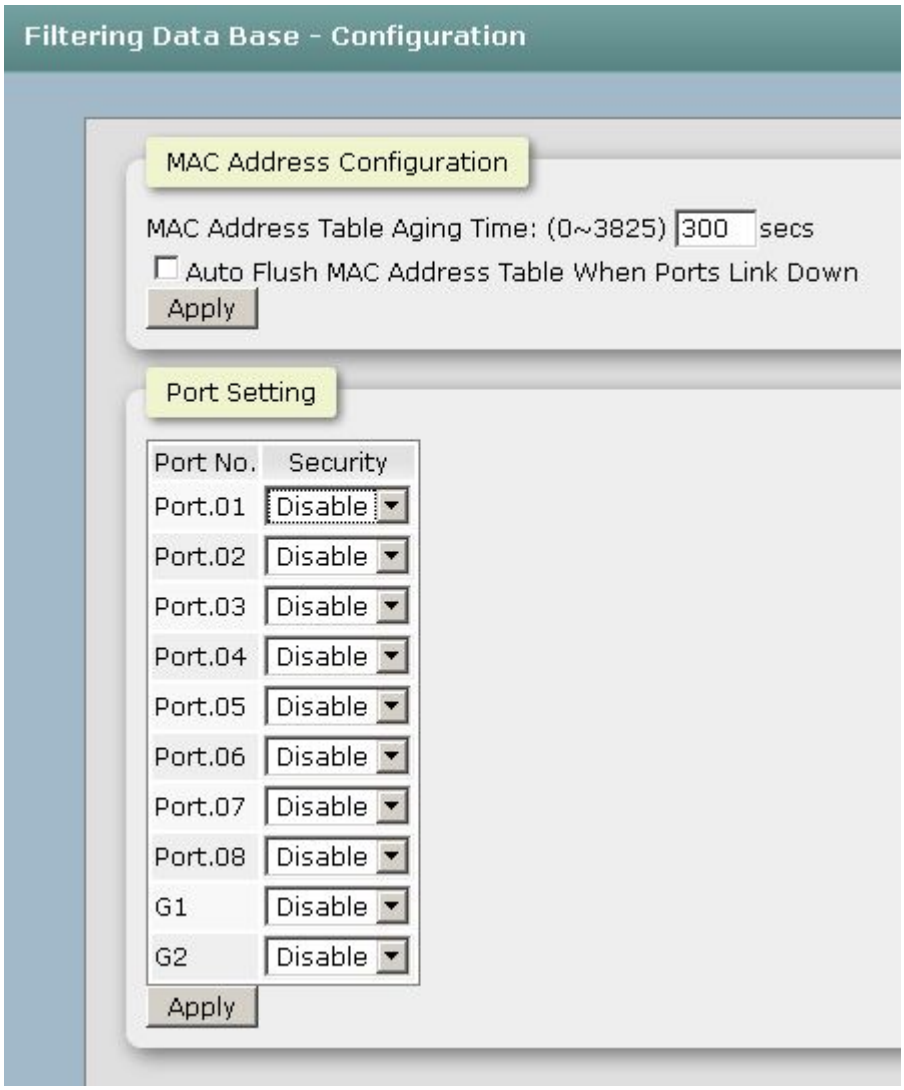
It will show you the information about Port Neighbor via LLDP protocol.

6.23 Filtering Database

Use the MAC address table to ensure the port security.

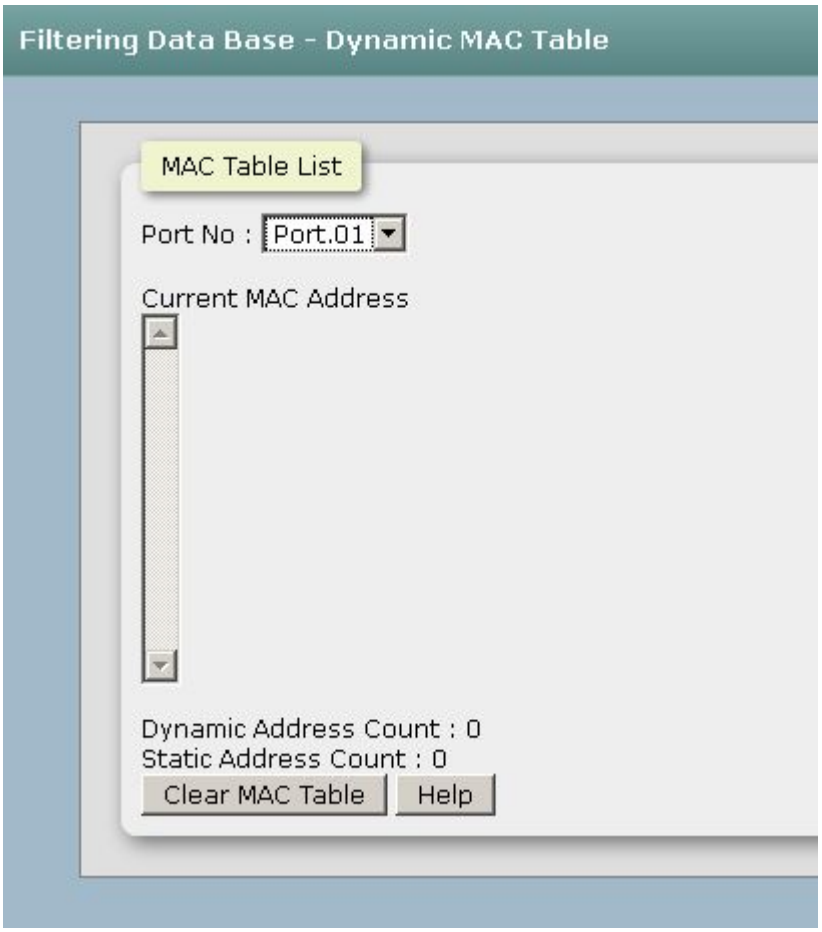
6.23.1 Configuration

- **MAC Address Configuration:**: Set the Aging time of MAC address table and define the event about port fail will influent the MAC table automatically or not.
- **Port Setting**: Define which port will be managed by Static MAC address table.
- Click Apply.



6.23.1 Dynamic MAC table

You can monitor the learning status of MAC address table in this function..



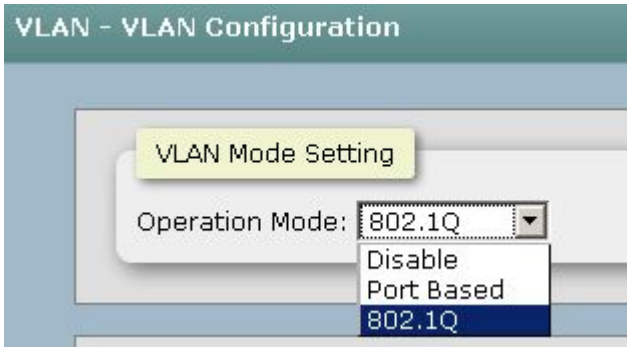
6.24 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN on a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

This switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".

6.24.1. VLAN Configuration

- **Operation Mode:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.



802.1Q VLAN Setting:

Enable GVRP mode and define the Management VLAN ID.

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

Port Setting:

Select the port you want to configure.

- **Link Type**: There are 4 types of link type.

  1. Access Link: A segment which provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

  Note: Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

  2. Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

  Note:

  A trunk port doesn't insert tag into an untagged frame, and therefore the

untagged VID column field is not available.
It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.
The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

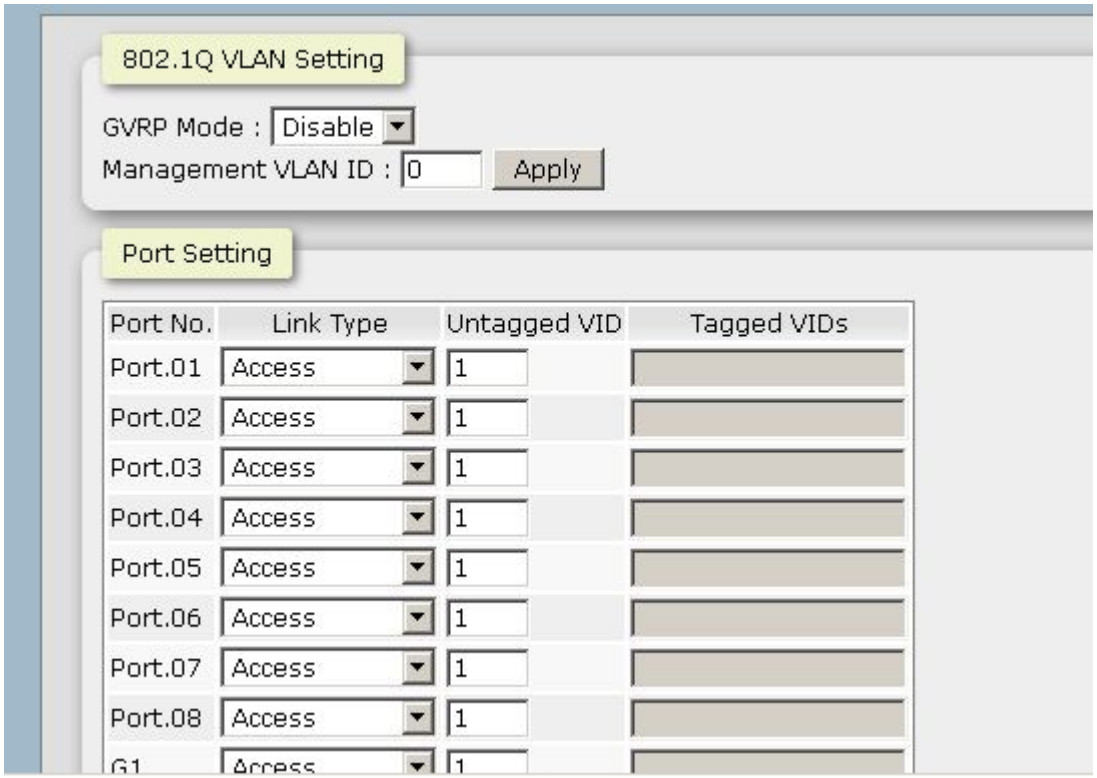
3. Hybrid Link: A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.

4. QinQ (Double Tag VLAN) configuration: Double Tag VLAN is another mechanism employed in a Metro LAN in which it can save IP v4 address by residing groups of sub-VLANs (customer port) in a VLAN(Host) and utilizing the default gateway IP address of Double Tag VLAN sharing the same IP subnet mask. Double Tag VLAN in L2 provides enhances security between customer (each home), by dis-communication between the sub-VLANs, even they are located in the same LAN and have the same IP subnet mask. Better yet, the configuration is simple than assigning each VLAN as per port based VLAN to customer (each home).

Note:

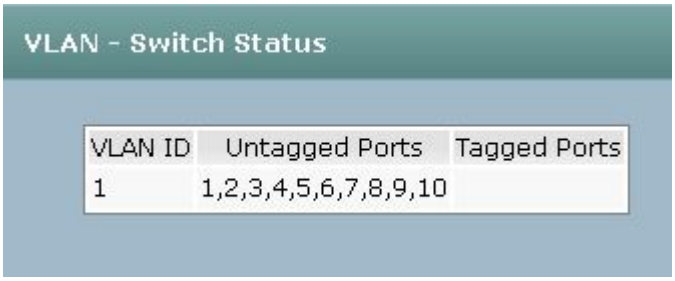
1. It's not necessary to type '1' in the tagged VID. The hybrid port will forward the frames of VLAN 1.
2. The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

- **Untagged VID:** This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- **Tagged VID:** This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- Click Apply to have the configuration take effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.



6.24.2 Switch Status

You can see the status of VLAN setting in this function..



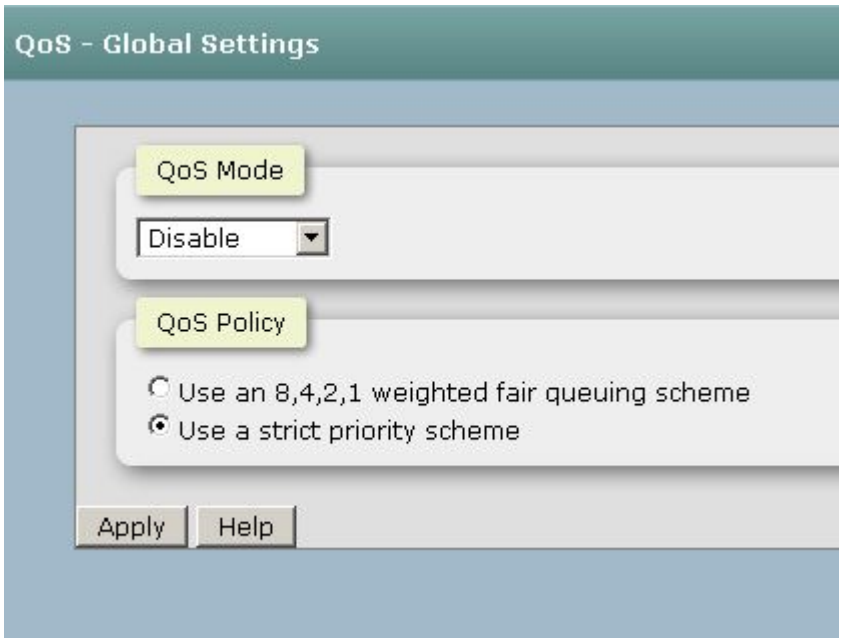
6.25 QoS

Quality of Service (QoS) is the ability to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP or Video Teleconferencing, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

6.25.1 Global Settings

Here you can choose to use an 8-4-2-1 queuing scheme or a strict priority scheme, or select the priority type to configure QoS policy.

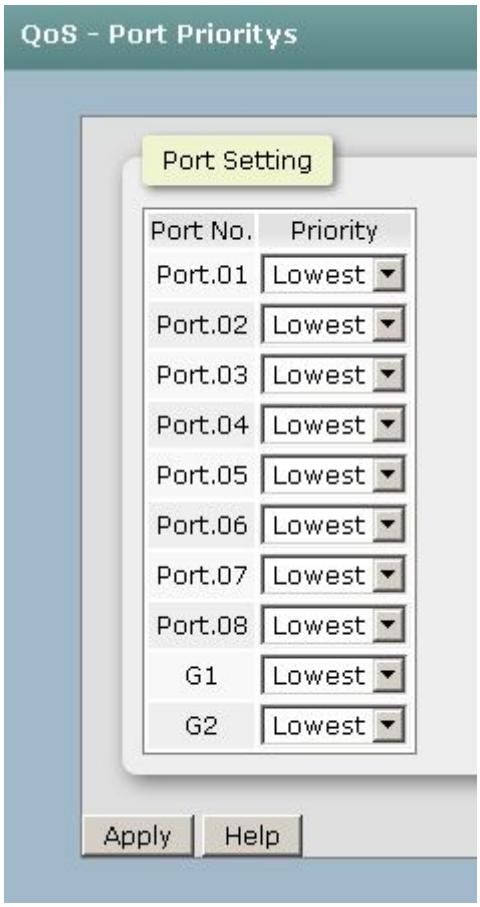
- **Qos Policy:** Select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use a strict priority scheme:** Always the higher queue will be processed first, except the higher queue is empty.
  - **Priority Type:** There are 5 priority type selections available—**Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. Disable means no priority type is selected.
- Click Apply to have the configuration take effect.



6.25.2 Port Priority

Configure the priority level for each port. With the drop-down selection item of **Priority Type** above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

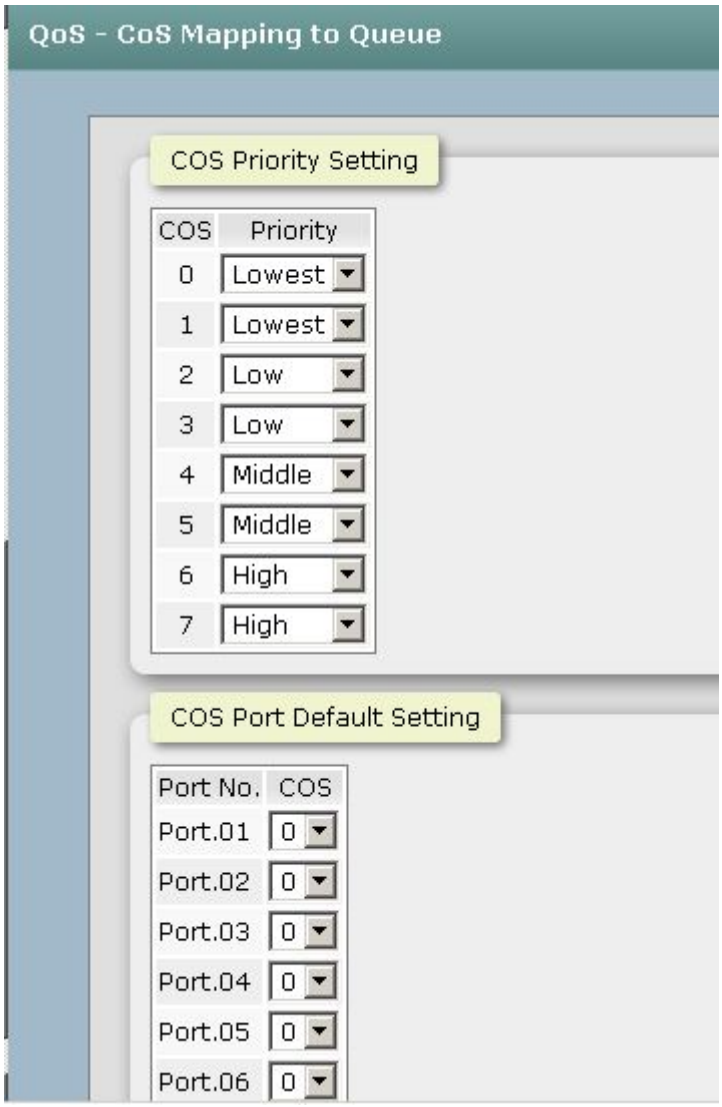
- **Port x:** Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.
- Click Apply to have the configuration take effect.



6.25.3 COS Mapping to Queue

Set up the COS priority level. With the drop-down selection item of **Priority Type** above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

- **COS priority:** Set up the COS priority level 0~7—High, Middle, Low, Lowest.
- Click Apply.



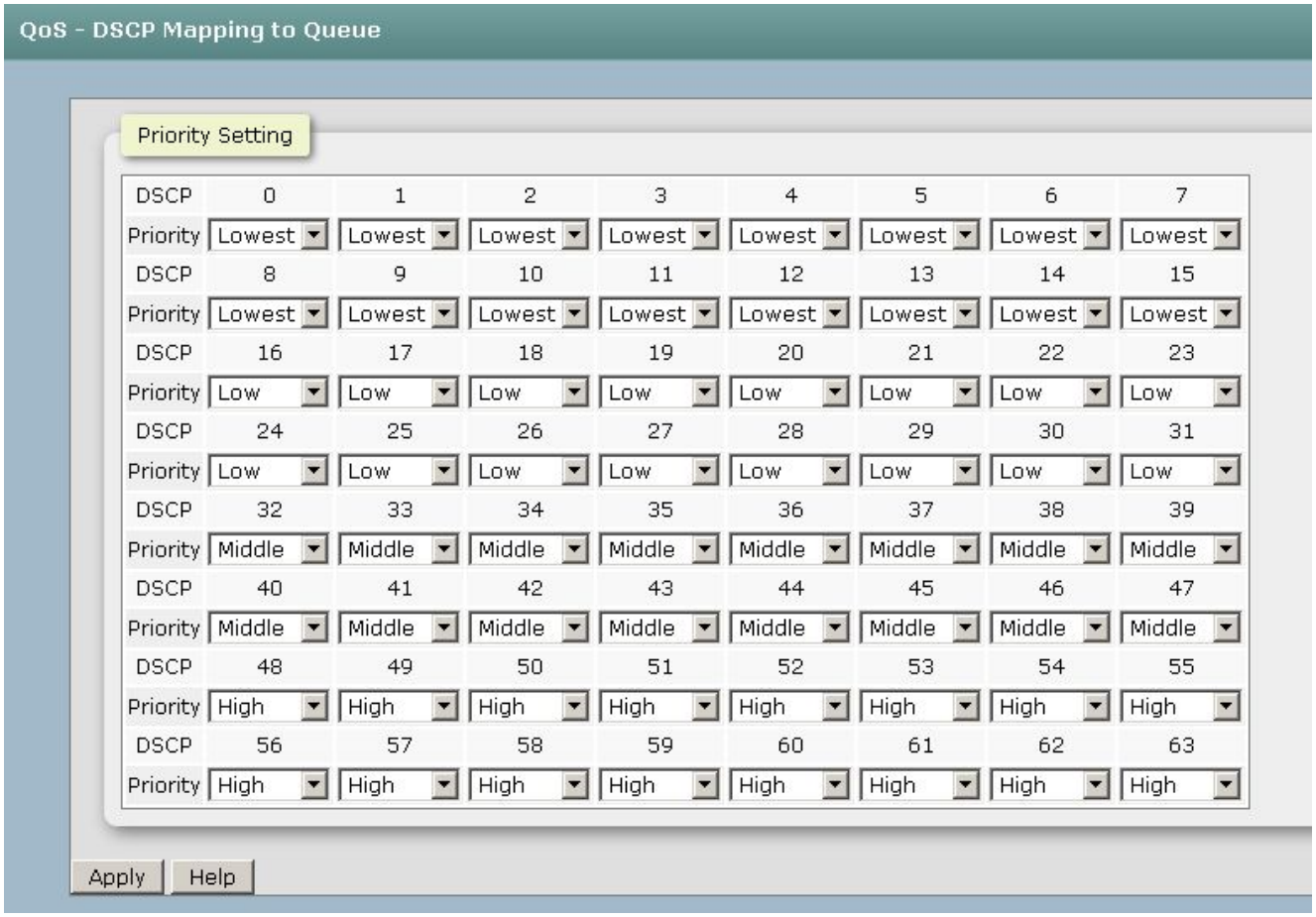
6.25.4 DSCP mapping to queue

Set up the DSCP priority. With the drop-down selection item of **Priority Type** above being selected as DSCP only/SDCP first, this control item will then be available to set the queuing policy for each port.

■ **DSCP priority:** The system provides 0~63 DSCP priority level. Each level has 4 types of priority—High, Middle, Low, and Lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the DSCP level value in the IP packet that has received. For example, the user sets the DSCP level 25 as high, the system will check the DSCP value of the received IP packet. If the DSCP

value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.

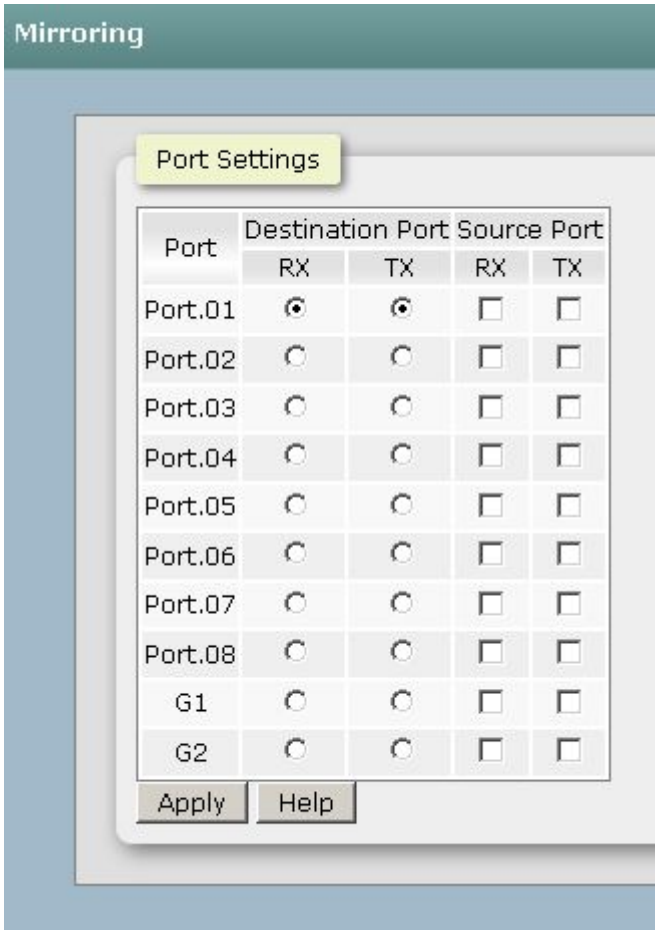
- Click Apply to have the configuration take effect.


QoS - DSCP Mapping to Queue
Priority Setting
DSCP 0 1 2 3 4 5 6 7
Priority Lowest Lowest Lowest Lowest Lowest Lowest Lowest Lowest
DSCP 8 9 10 11 12 13 14 15
Priority Lowest Lowest Lowest Lowest Lowest Lowest Lowest Lowest
DSCP 16 17 18 19 20 21 22 23
Priority Low Low Low Low Low Low Low Low
DSCP 24 25 26 27 28 29 30 31
Priority Low Low Low Low Low Low Low Low
DSCP 32 33 34 35 36 37 38 39
Priority Middle Middle Middle Middle Middle Middle Middle Middle
DSCP 40 41 42 43 44 45 46 47
Priority Middle Middle Middle Middle Middle Middle Middle Middle
DSCP 48 49 50 51 52 53 54 55
Priority High High High High High High High High
DSCP 56 57 58 59 60 61 62 63
Priority High High High High High High High High
Apply
Help

6.25. Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port, which means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

- **Destination Port:** There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray.
- **Source Port:** The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.
- And then, click Apply button.



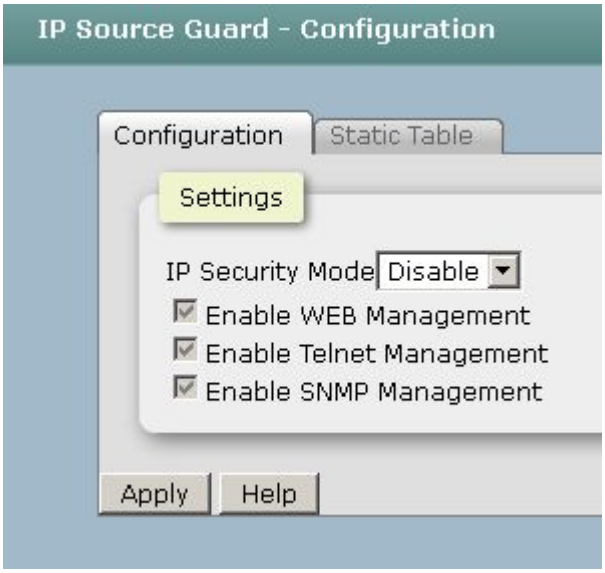
6.26. Security

You can block the un-authorized client in this function.

6.26.1 IP Source Guard - Configuration

IP Source Guard function allows the user to assign 10 specific IP addresses that have permission to manage the switch through the http and telnet services for the securing switch management. The purpose of giving the limited IP addresses permission is to allow only the authorized personnel/device can do the management task on the switch.

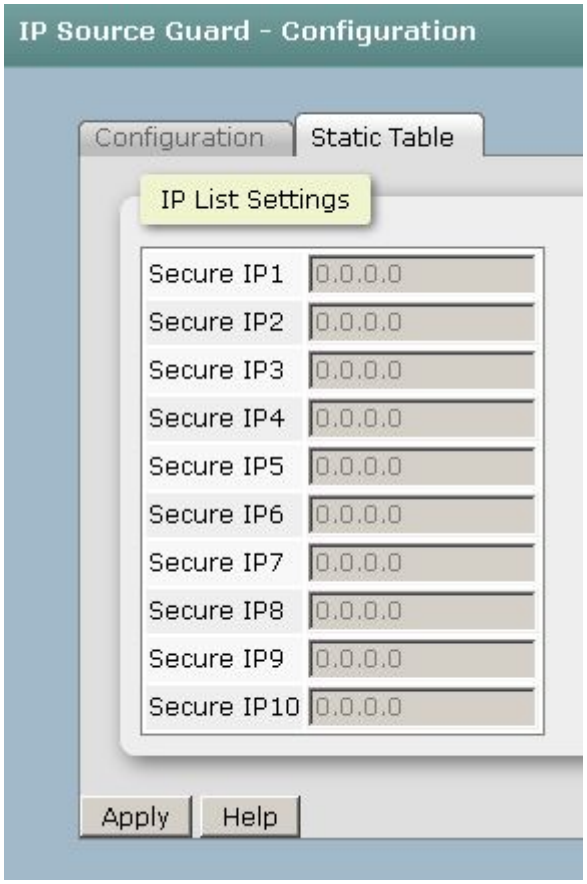
- **IP Security Mode:** Having set this selection item in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via HTTP service.
- **Enable Telnet Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via telnet service.
- **Enable SNMP Management:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via SNMP service.



6.26.2 IP Source Guard – Static Table

- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service once **IP Security Mode** is enabled.
- And then, click Apply to have the configuration take effect.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.

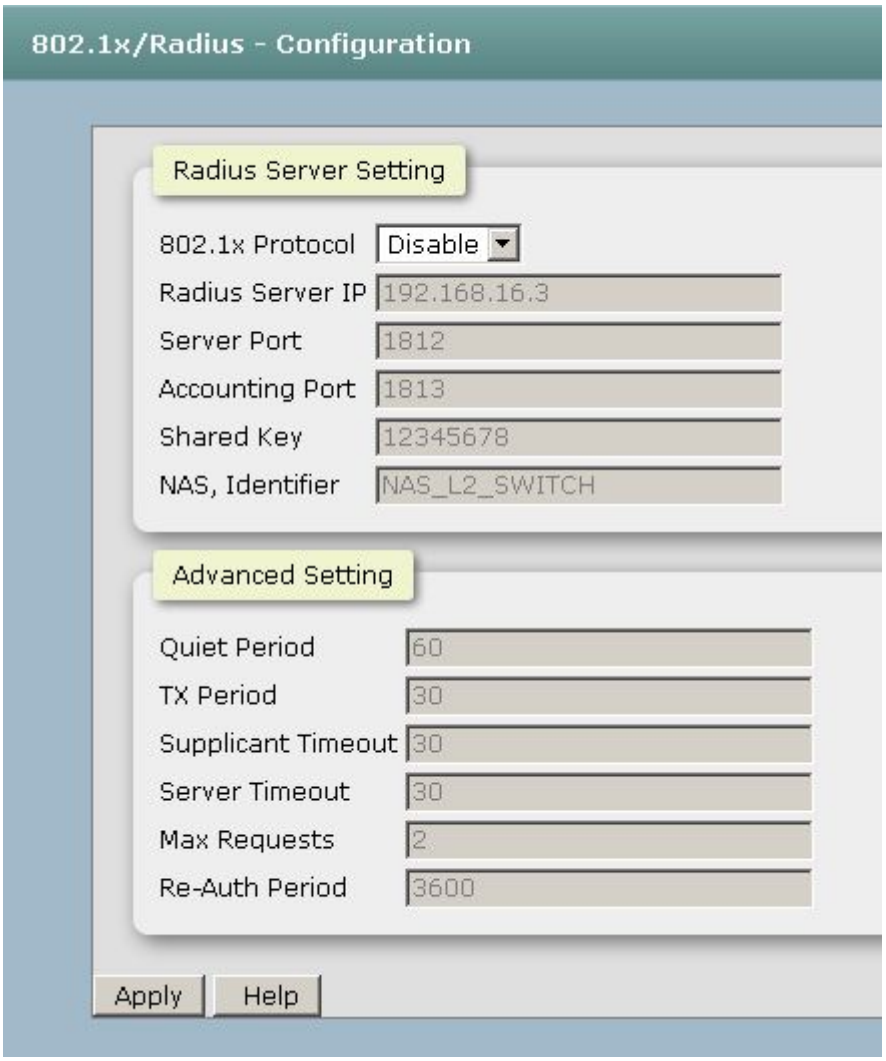


6.26.3 802.1X/Radius

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).
After enabling the IEEE 802.1X function, you can configure the parameters of this function.

6.26.3.1 Configuration

- **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time which clients connected must be re-authenticated.
- Click Apply.

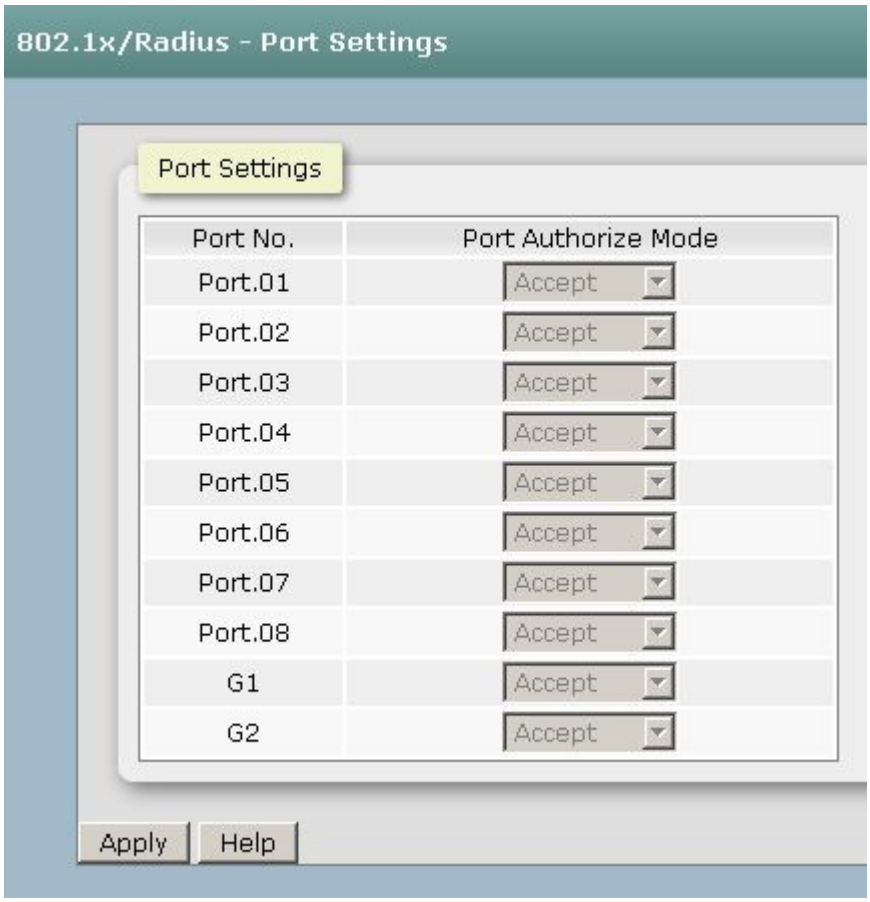


6.26.3.2 Port Setting

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

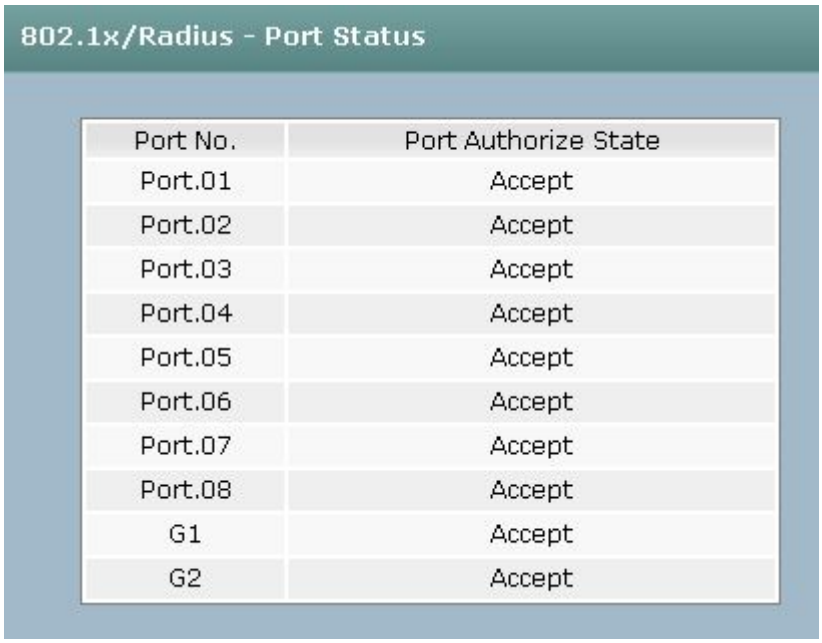
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the authorized state.
- **Authorize:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.

- Click Apply.



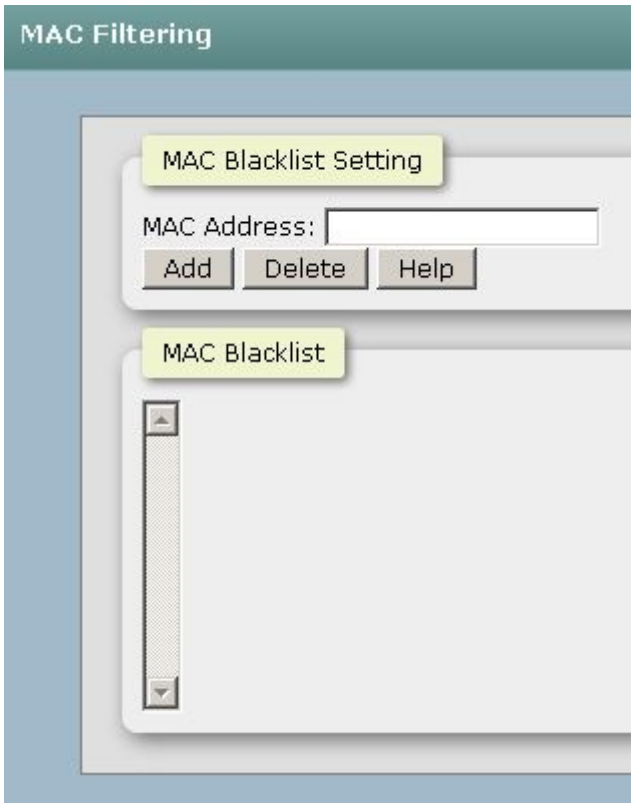
6.26.3.3 Port Status

You can monitor the port Authorized state in this function.


802.1x/Radius - Port Status
Port No.
Port Authorize State
Port.01
Accept
Port.02
Accept
Port.03
Accept
Port.04
Accept
Port.05
Accept
Port.06
Accept
Port.07
Accept
Port.08
Accept
G1
Accept
G2
Accept

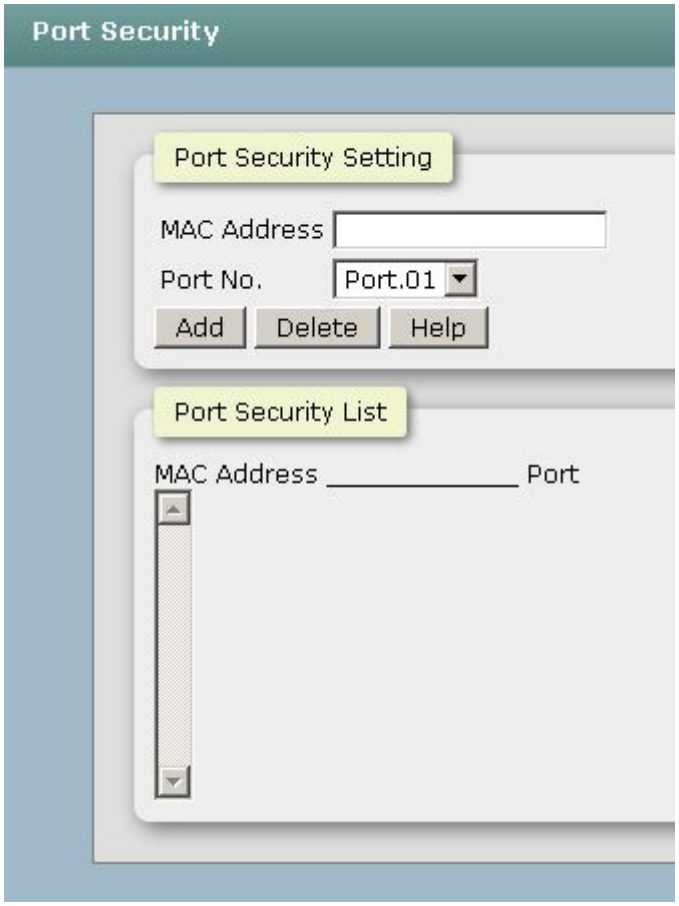
6.26.4 MAC Filtering

You can block the un-authorized MAC by switch in this function.



6.26.5 Port Security

You can block the un-authorized MAC by oer port in this function.



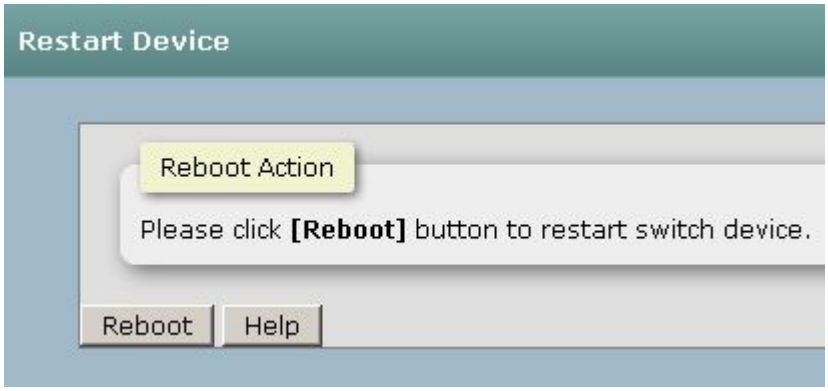
6.27. Maintenance

6.27.1 Save Configuration

Save the current setting of switch ..

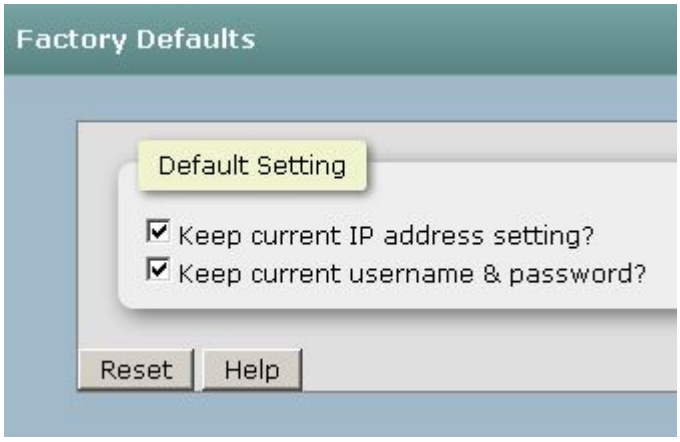
6.27.2 Restart Device

Make the switch warm start.



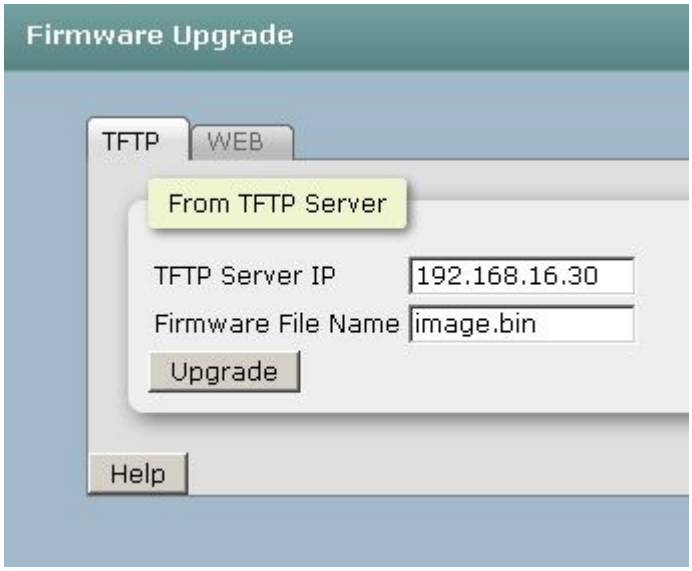
6.27.3 Factory Defaults

Reset switch to default configuration. Click “Reset” to reset all configurations to the default value.



6.27.4 Firmware Upgrade

- **TFTP Server IP Address:** Type in your TFTP server IP.
- **Firmware File Name:** Type in the name of the firmware image file to be updated.
- Click Upgrade

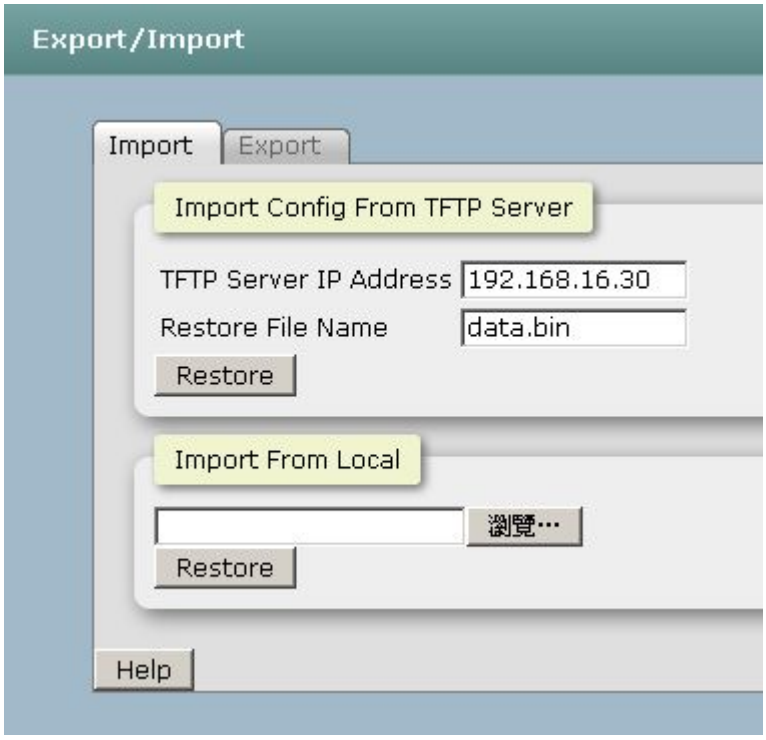


You can also browser the firmware on your hard drive by web update.

6.27.5 Export/Import

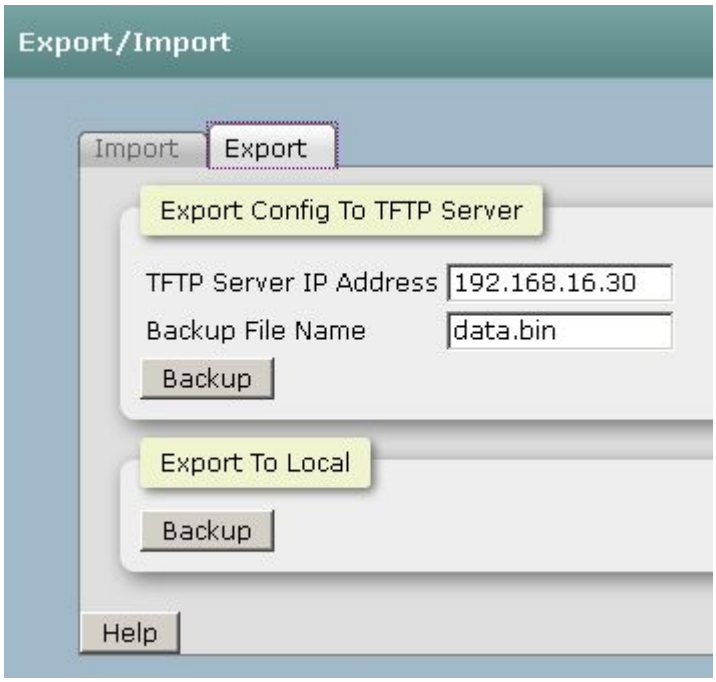
You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the switch will download back the flash image.

- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Restore File Name:** Type in the correct file name for restoring.
- Click Restore



You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

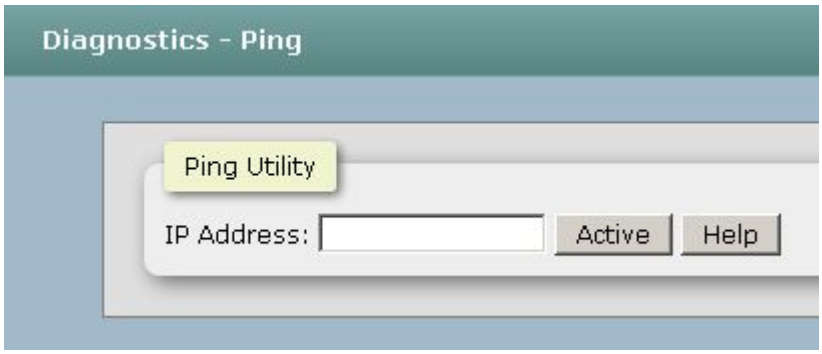
- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Backup File Name:** Type in the file name.
- Click Backup..



6.27.6 Diagnostics

6.27.6.1 Ping

You can ping other network device in this function.

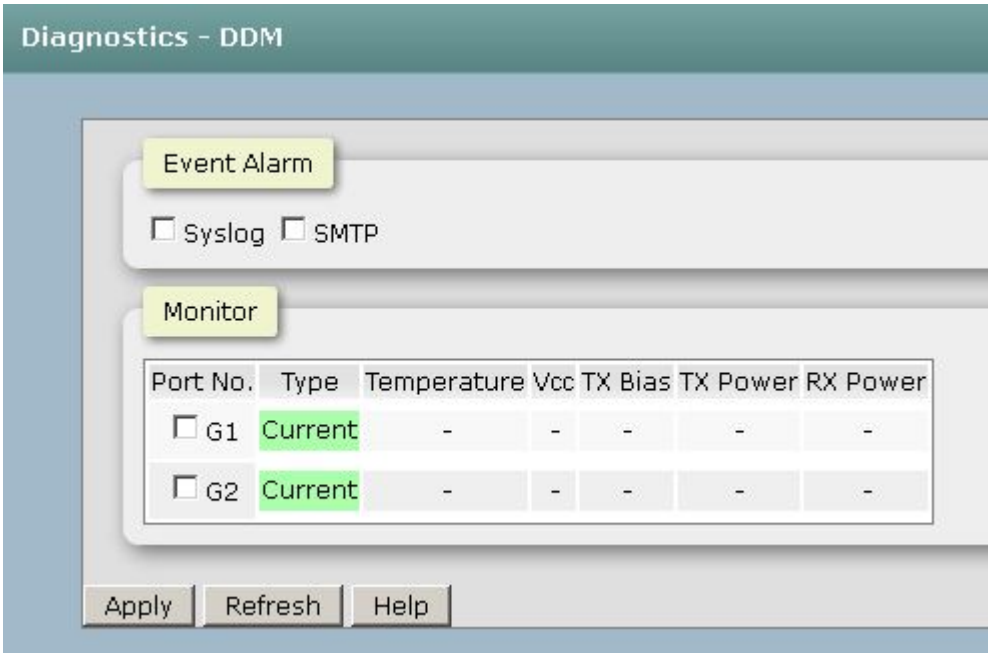


6.27.6.2 DDM

Port No.: Specify the SFP port and show the SFP module information.

- **Temperature:** Display the internal temperature of the SFP default threshold and present value.

- **Vcc:** Display the supply voltage of the SFP default threshold and present value.
- **Tx Bias:** Display the Bias current of the SFP default threshold and present value.
- **TX PWR:** Display the transmission power of the SFP default threshold and present value.
- **RX PWR:** Display the received power of the SFP default threshold and present value.
- **Syslog/SMTP:** The port will send an e-mail or log on local to administrator when detecting the exceptional value.



Troubles shooting

- Verify that is using the right power cord/adapter (DC 24-48V), please don't use the power adapter with DC output higher than 48V, or it may damage this device.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100 Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators:** To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.

Appendix A—RJ-45 Pin Assignment

RJ-45 Pin Assignments

The UTP/STP ports will automatically sense for Fast Ethernet (10Base-T/100Base-TX connections), or Gigabit Ethernet (10Base-T/100Base-TX/1000Base-T connections). Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the figures below for straight through and crossover cable schematic.

■ 10 /100BASE-TX Pin outs

With10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

■ RJ-45 Pin Assignments

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

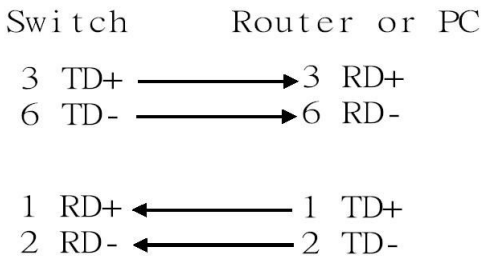
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

The table below shows the 10/100BASE-TX MDI and MDI-X port pin outs.

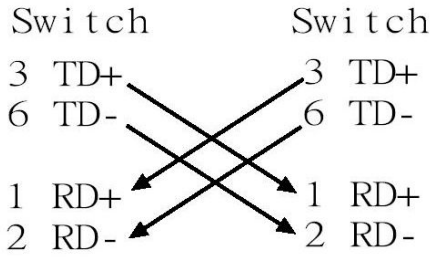
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

10/100Base-TX Cable Schematic

The following two figures show the 10/100Base-TX cable schematic.



Straight-through cable schematic

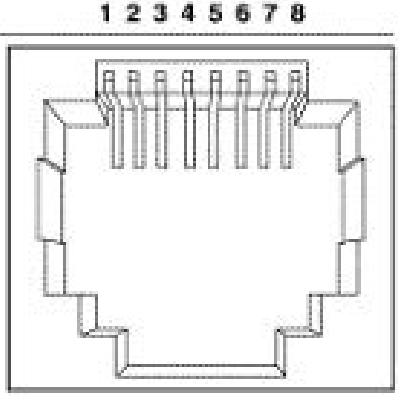


Cross over cable schematic

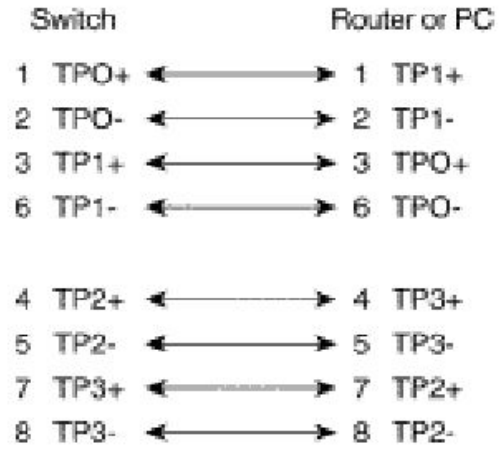
10/100/1000Base-TX Pin outs

The following figure shows the 10/100/1000 Ethernet RJ-45 pin outs.

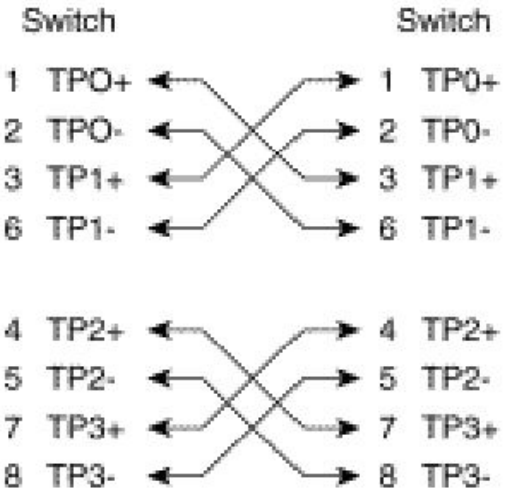
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

RJ-45 Pin Assignment of PoE

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data; pins 4, 5, 7 and 8 are used for power supplying.

Pin out of Cisco non-802.3af standard PD

Pin	Signal
1	RX+
2	RX-
3	TX+
4	VCC -
5	VCC -
6	TX-
7	VCC +
8	VCC +

Pin out of PoE Midspan Hub/Switch

Pin	Signal / Name
1	RX+
2	RX-
3	TX+
4	VCC+
5	VCC+
6	TX-
7	VCC-
8	VCC-

■ Pin out of PoE Endspan Hub/Switch

Pin	Signal / Name
1	TX+/VCC+
2	TX-/VCC+
3	TX+/VCC-
4	
5	
6	TX-/VCC-
7	
8	

Note ‘+’ and ‘-‘ signs represent the polarity of the wires that make up each wire pair. Before you power PD, please check the RJ-45 connector pin assignment follow IEEE802.3af standard; otherwise you may need to change one of the RJ-45 connector pin assignment attached with the UTP cable.

Appendix B—Command Sets

Commands Set List

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

Netstar Commands	Level	Description	Example
enable	**E**	Enter Privileged EXEC mode	switch>**enable**
quit	**E**	Logout command line shell	switch>**quit**
show	**E**	Show switch configuration	switch>**show config**
uptime	**E**	Show system up time	switch>**uptime**
disable	**P**	Leave Privileged EXEC mode	switch>enable switch#**disable**
configure	**P**	Enter Global configuration mode	switch>enable switch#**configure**
end	**G**	Leave Global configuration mode	switch>enable switch(config)#**end**
exit	**G**	Leave Global configuration mode	switch>enable switch(config)#**exit**

Switch Setting Commands Set

Netstar Commands	Level	Description	Example
show terminal	**P**	Show console information	switch>enable switch#**show terminal**
system name **[System Name]**	**G**	Configure system name	switch>enable switch#configure

			switch(config)#**system name xxx**
system location [System Location]	**G**	Set switch system location string	switch>enable switch#configure switch(config)#**system location xxx**
system description [System Description]	**G**	Set switch system description string	switch>enable switch#configure switch(config)#**system description xxx**
system contact [System Contact]	**G**	Set switch system contact window string	switch>enable switch#configure switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**

Admin Password Commands Set

Netstar Commands	Level	Description	Example
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch>enable switch#configure switch(config)#**admin username xxxxxx**
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch>enable switch#configure switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch>enable switch#**show admin**

IP Setting Commands Set

Netstar Commands	Level	Description	Example
ip address [Ip-address] [Subnet-	**G**	Configure the IP address of switch	switch>enable switch#configure

mask] [Gateway]			switch(config)#**ip address 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch>enable switch#configure switch(config)#**ip dhcp**
show ip	**P**	Show IP information of switch	switch>enable switch#**show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch>enable switch#configure switch(config)#**no ip dhcp**

SNTP Commands Set

Netstar Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch>enable switch#configure switch(config)#**sntp enable**
sntp ip [IP]	**G**	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch>enable switch#configure switch(config)#**sntp ip 192.168.16.1**
sntp timezone [Timezone] Format: [1~63]	**G**	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch>enable switch#configure switch(config)#**sntp timezone 22**
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this	switch>enable switch#configure switch(config)#**sntp daylight**

		command can't be applied.	
sntp daylight-period **[Start time] [End time] Format:[yyyymmdd-hh:mm]**	**G**	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch>enable switch#configure switch(config)# **sntp daylight-period 20120808-01:01 20120809-01:01**
ntp daylight-offset **[Minute]**	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch>enable switch#configure switch(config)#**sntp daylight-offset 60**
show sntp	**P**	Show SNTP information	switch>enable switch#**show sntp**
show sntp timezone	**P**	Show index number of time zone list	switch>enable switch#**show sntp timezone**
no sntp	**G**	Disable SNTP function	switch>enable switch#configure switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch>enable switch#configure switch(config)#**no sntp daylight**

LLDP Commands Set

Netstar Commands	Level	Description	Example
lldp enable	**G**	Enable LLDP function	switch>enable switch#configure switch(config)# **lldp enable**
lldp interval **[TIME sec]**	**G**	Configure LLDP interval	switch>enable switch#configure

			switch(config)#**lldp interval 1800**
lldp synctime [enable|disable]	**G**	Enable/disable LLDP sync time	switch>enable switch#configure switch(config)#**lldp synctime enable**
show lldp	**P**	Show LLDP information	switch>enable switch#**show lldp**
no lldp	**G**	Disable LLDP	switch>enable switch#configure switch(config)#**no lldp**

Backup & Restore Commands Set

Netstar Commands	Level	Description	Defaults Example
tftp [server IP] **backup** [file name]	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# **tftp 192.168.16.120 backup 123.bin**
tftp [server IP] **restore** [file name]	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# **tftp 192.168.16.120 restore 123.bin**

Upgrade Firmware Commands Set

Netstar Commands	Level	Description	Defaults Example
tftp [server IP] **upgrade** [file name]	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch>enable switch#configure switch(config)# **tftp 192.168.16.120 upgrade image.bin**

DHCP Server Commands Set

Netstar Commands	Level	Description	Example
dhcpserver enable	**G**	Enable DHCP Server	switch>enable switch#configure switch(config)#**dhcpserver enable**
dhcpserver lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch>enable switch#configure switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch>enable switch#configure switch(config)#**dhcpserver highip 192.168.1.200**
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch>enable switch#configure switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch>enable switch#configure switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch>enable switch#configure switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime **[Hours.]**	**G**	Configure lease time (Hours.)	switch>enable switch#configure switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch>enable switch#configure

			switch(config)#interface fastEthernet 2 switch(config-if)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch>enable switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch>enable switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch>enable switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch>enable switch#configure switch(config)#**no dhcpserver**

Port Control Commands Set

Netstar Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch>enable switch#configure switch(config)#**interface fastEthernet 2**
state **[enable|disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch>enable switch#configure switch(config)#interface fastEthernet 2 (config-if)#**state disable**
duplex **[full | half]**	**I**	Use the duplex configuration	switch>enable switch#configure

		command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#**duplex full**
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**speed 100**
flowcontrol mode [symmetric|asymmetric]	**I**	Configure flow control	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **flowcontrol mode asymmetric**
no flowcontrol	**I**	Disable flow control of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **no flowcontrol**
security enable	**I**	Enable security of interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**security enable**
no security	**I**	Disable security of interface	switch>enable switch#configure switch(config)#interface

			fastEthernet 2 switch(config-if)#**no security**
auto-sfp **[Enable|Disable]**	**G**	Enable/disable to auto detect 100/1000 SFP	switch>enable switch#configure switch(config)#**auto-sfp disable**
alias[name]	**I**	Set port alias name	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**alias 1111**
show interface configuration	**I**	show interface configuration status	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**show interface configuration**

Port Status Commands Set

Netstar Commands	Level	Description	Example
show interface status	**I**	show interface actual status	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch (config-if)#**show interface status**

Rate Limit Commands Set

Netstar Commands	Level	Description	Example
ratelimit type all	**I**	Set interface ingress limit frame type to “accept all frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit type all**

ratelimit type broadcast-multicast-flooded-unicast	**I**	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit type broadcast-multicast-flooded-unicast**
ratelimit type broadcast-multicast	**I**	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit type broadcast-multicast**
ratelimit type broadcast-only	**I**	Set interface ingress limit frame type to “only accept broadcast frame”	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit type broadcast-only**
ratelimit in **[kbps]**	**I**	Set interface input bandwidth. zero means no limit.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit in 160**
ratelimit out **[kbps]**	**I**	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **ratelimit out 160**

show ratelimit	**I**	Show interfaces bandwidth control	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**show ratelimit**

Trunk Commands Set

Netstar Commands	Level	Description	Example
aggregator priority [1~65535]	**G**	Set port group system priority	switch>enable switch#configure switch(config)#**aggregator priority 22**
aggregator group [GroupID] [Port-list] **lacp workp** [Workport]	**G**	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch>enable switch#configure switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator activityport [Group ID] [Port Numbers]	**G**	Set activity port	switch>enable switch#configure switch(config)#**aggregator activityport 1 2**

aggregator group [GroupID] [Port-list] **nolacp**	**G**	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch>enable switch#configure switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	**P**	Show the information of trunk group	switch>enable switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	**G**	Disable the LACP function of trunk group	switch>enable switch#configure switch(config)#**no aggregator lacp 1**
no aggregator group [GroupID]	**G**	Remove a trunk group	switch>enable switch#configure switch(config)#**no aggregator group 1**

PRO-RING IIS Commands Set

Netstar Commands	Level	Description	Example
prorstp enable	**I**	Enable PRO-RING IIS for this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **prorstp enable**
prorstp-root	**G**	Configure PRO-RING	switch>enable

[disable|enable|backup]		IIS ROOT	switch#configure switch(config)#**prorstp-root enable**
no prorstp	**I**	Disable PRO-RING IIS for this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **no prorstp**
no prorstp	**G**	Disable PRO-RING IIS for all interfaces	switch>enable switch#configure switch(config)# **no prorstp**
show prorstp	**P**	Show PRO-RING IIS configuration	switch>enable switch#**show prorstp**

RSTP Commands Set

Netstar Commands	Level	Description	Example
rstp enable	**G**	Enable RSTP	switch>enable switch#configure switch(config)#**rstp enable**
rstp priority [0~61440]	**G**	Configure RSTP bridge priority parameter	switch>enable switch#configure switch(config)#**rstp priority 4096**
rstp max-age [6~40]	**G**	Configure RSTP max age parameter	switch>enable switch#configure switch(config)#**rstp max-age 6**
rstp hello-time [1~10]	**G**	Configure RSTP hello time parameter.	switch>enable switch#configure switch(config)#**rstp hello-time 1**
rstp forward-time [4~30]	**G**	Configure RSTP forward time parameter.	switch>enable switch#configure switch(config)#**rstp forward-time 4**

rstp path-cost [0:auto,1-200000000]	**I**	Path cost on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**rstp path-cost 20**
rstp port-priority [0-240]	**I**	Port priority on this interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **rstp port-priority 16**
rstp admin-p2p [Auto|True|False]	**I**	Admin P2P on this interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**rstp admin-p2p false**
rstp admin-edge [True|False]	**I**	Admin Edge on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**rstp admin-edge false**
rstp admin-non-stp [True|False]	**I**	Admin NonSTP on this interface	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**rstp admin-non-stp false**
show rstp	**G**	Show RSTP information.	switch>enable switch#**show rstp**

no rstp	**G**	Disable RSTP.	switch>enable switch#configure switch(config)#**no rstp**

VLAN Commands Set

Netstar Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch>enable switch#**vlan database**
vlanmode [portbase| 802.1q | diable| gvrp]	**V**	To set switch VLAN mode.	switch>enable switch#vlan database switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode disable** or switch(vlan)#**vlanmode gvrp**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	**V**	Add new port based VALN	switch>enable switch#vlan database switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch>enable switch#vlan database switch(vlan)#**show vlan 2**
no vlan [VID]	**V**	Delete port base group ID	switch>enable switch#vlan database switch(vlan)#**no vlan 2**
IEEE 802.1Q VLAN			

vlan 8021q mnt-vid [VID]	**V**	Configure management VID (0 is disabled)	switch>enable switch#vlan database switch(vlan)#**vlan 8021q mnt-vid 22**
vlan 8021q name [GroupName] **vid** [VID]	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch>enable switch#vlan database switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)#**vlan 8021q port 3 access-link untag 22**
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch>enable switch#vlan database switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q port [PortNumber] **hybrid-link-qinq untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a qinq link for VLAN by port, if the port belong to a trunk group, this command	switch>enable switch#vlan database switch(vlan)#**vlan 8021q port 3 hybrid-link-qinq untag 4 tag**

		can't be applied.	**3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link-qinq untag 5 tag 6-8**
vlan 8021q aggreator **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)# **vlan 8021q aggreator 3 access-link untag 33**
vlan 8021q aggreator **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)#**vlan 8021q aggreator 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q aggreator 3 trunk-link tag 3-20**
vlan 8021q aggreator **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)#**vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8**
vlan 8021q aggreator **[PortNumber]** **hybrid-link-qinq untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a qinq link for VLAN by trunk group	switch>enable switch#vlan database switch(vlan)#**vlan 8021q aggreator 3 hybrid-link-qinq untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q**

			aggreator 3 hybrid-link-qinq untag 5 tag 6-8
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch>enable switch#vlan database switch(vlan)#**show vlan 2**
no vlan [GroupID]	**V**	Delete port base group ID	switch>enable switch#vlan database switch(vlan)#**no vlan 2**

SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp agent-mode [v1v2c|v3]	**G**	Select the agent mode of SNMP	switch>enable switch#configure switch(config)#**snmp agent-mode v1v2c**
snmp community-strings [Community] **right** [RO/RW]	**G**	Add SNMP community string.	switch>enable switch#configure switch(config)#**snmp community-strings public right rw**
Snmp trap server [IP address] **community** [Community-string] **trap-version** [v1|v2c]	**G**	Configure SNMP server host information and community string	switch>enable switch#configure switch(config)# **snmp trap server 192.168.1.120 community public trap-version v2c**
snmp snmpv3-user [UserID] **password** [Authentication Password] [Privacy Password]	**G**	Create a SNMPv3 user profile	switch>enable switch#configure switch(config)#**snmp snmpv3-user root password 123 123**

no snmp community-strings [Community]	**G**	Disable SNMP community strings function	switch>enable switch#configure switch(config)#**no snmp community-strings public**
no snmp trap server [IP Address]	**G**	Remove SNMP trap setting	switch>enable switch#configure switch(config)#**no snmp trap server 192.168.1.120**
no snmp snmpv3-user password [Authentication Password] [Privacy Password]	**G**	Remove SNMPv3 user profile	switch>enable switch#configure switch(config)#**no snmp snmpv3-user root password 123 123**

Traffic Prioritization Commands Set

Netstar Commands	Level	Description	Example
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	**G**	Setting of QOS priority type	switch>enable switch#configure switch(config)#**qos prioritytype port-base**
qos policy [weighted-fair|strict]	**G**	Select QOS policy scheduling	switch>enable switch#configure switch(config)#**qos policy weighted-fair**
qos priority portbased [Port] [lowest|low|middle|high]	**G**	Configure Port-based Priority	switch>enable switch#configure switch(config)#**qos priority portbased 1 low**
qos priority cos [Priority][lowest|low|middle|high]	**G**	Configure COS Priority	switch>enable switch#configure switch(config)#**qos priority cos 0 middle**

qos priority cosportdefault [Port][Priority]	**G**	Configure COS Port default	switch>enable switch#configure switch(config)#**qos priority cosportdefault 1 1**
qos priority tos [Priority][lowest|low|middle|high]	**G**	Configure TOS Priority	switch>enable switch#configure switch(config)#**qos priority tos 3 high**
show qos	**P**	Displays the information of QoS configuration	switch>enable switch#configure switch#**show qos**
no qos	**G**	Disable QoS function	switch>enable switch#configure switch(config)#**no qos**

IGMP Commands Set

Netstar Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch>enable switch#configure switch(config)#**igmp enable**
igmp query [auto/fource]	**G**	Configure IGMP query mode	switch>enable switch#configure switch(config)#**igmp query auto**
igmp unregister [flooding/blocking/sourceonly]	**G**	Configure IGMP unregister stream	switch>enable switch#configure switch(config)#**igmp unregister flooding**
igmp last-query-count [1~2 sec.]	**G**	Configure Last Member Query Count	switch>enable switch#configure switch(config)# **igmp last-query-count 1**
igmp last-query-interval [1~250 tenths of a sec.]	**G**	Configure Last Member Query Interval	switch>enable switch#configure switch(config)# **igmp last-query-**

			interval 100
igmp query-interval **[1~250 sec.]**	**G**	Configure Query Interval	switch>enable switch#configure switch(config)# **igmp query-interval 100**
query-response-interval **[1~250 tenths of a sec.]**	**G**	Configure Query Response Interval	switch>enable switch#configure switch(config)# **igmp query-response-interval 100**
show igmp configuration	**P**	Show IGMP configuration.	switch>enable switch#**show igmp configuration**
show igmp table	**P**	Show IGMP snooping table.	switch>enable switch#**show igmp table**
no igmp	**G**	Disable IGMP snooping function	switch>enable switch#configure switch(config)#**no igmp**
no igmp query	**G**	Disable IGMP query	switch>enable switch#configure switch(config)#**no igmp query**

Multicast Static Filtering Table Commands Set

Netstar Commands	Level	Description	Example
multicast-filtering **[IP_addr]**	**I**	Configure multicast filtering entry of interface.	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config)# **multicast-filtering 225.100.100.100**
no multicast-filtering **[IP_addr]**	**I**	Remove multicast filtering entry of interface	switch>enable switch#configure switch(config)#interface

			fastEthernet 2 switch(config-if)#**no multicast-filtering 225.100.100.100**
show multicast-filtering	**P**	Show multicast filtering table	switch>enable switch# **show multicast-filtering**

IP Security Commands Set

Netstar Commands	Level	Description	Example
security enable	**G**	Enable IP security function	switch>enable switch#configure switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch>enable switch#configure switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch>enable switch#configure switch(config)#**security telnet**
security snmp	**G**	Enable IP security of SNMP server	switch>enable switch#configure switch(config)#**security snmp**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch>enable switch#configure switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch>enable switch#**show security**
no security	**G**	Disable IP security function	switch>enable switch#configure switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch>enable switch#configure switch(config)#**no security http**

no security telnet	**G**	Disable IP security of telnet server	switch>enable switch#configure switch(config)#**no security telnet**
no security snmp	**G**	Disable IP security of SNMP server	switch>enable switch#configure switch(config)#**no security snmp**

Port Security Commands Set

Netstar Commands	Level	Description	Example
mac-address-table static hwaddr [HW-Addr]	**I**	Configure MAC address entry of interface (static).	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**mac-address-table static hwaddr 000012345678**
show mac-address-table static	**P**	Show MAC address table (static)	switch>enable switch#**show mac-address-table static**
no mac-address-table static hwaddr [HW-Addr]	**I**	Remove an entry of MAC address table of interface (static)	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**no mac-address-table static hwaddr 000012345678**

MAC Blacklist Commands Set

Netstar Commands	Level	Description	Example
mac-address-table filter hwaddr [HW-Addr]	**G**	Configure MAC address entry of interface (filter)	switch>enable switch#configure switch(config)#**mac-address-table filter hwaddr 000012348678**

show mac-address-table filter	**P**	Show MAC address table (filter).	switch>enable switch#**show mac-address-table filter**
no mac-address-table filter hwaddr [HW-Addr]	**G**	Remove an entry of MAC address table (filter)	switch>enable switch#configure switch(config)#**no mac-address-table filter hwaddr 000012348678**

802.1x Commands Set

Netstar Commands	Level	Description	Example
8021x enable	**G**	Enable IEEE802.1x function	switch>enable switch#configure switch(config)# **8021x enable**
8021x system radiusip [Radius Server IP]	**G**	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch>enable switch#configure switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [Port Number]	**G**	Use the 802.1x system server port global configuration command to change the radius server port	switch>enable switch#configure switch(config)# **8021x system serverport 1815**
8021x system accountport [Port Number]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch>enable switch#configure switch(config)# **8021x system accountport 1816**
8021x system sharedkey [SharedKey]	**G**	Use the 802.1x system share key global configuration command to change	switch>enable switch#configure switch(config)# **8021x system sharedkey 123456**

		the shared key value.	
8021x system nasid [NAS ID]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch>enable switch#configure switch(config)# **8021x system nasid test1**
8021x misc quietperiod [Seconds]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch>enable switch#configure switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [Seconds]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch>enable switch#configure switch(config)# **8021x misc txperiod 5**
8021x misc supptimeout [Seconds]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch>enable switch#configure switch(config)# **8021x misc supptimeout 20**
8021x misc servertimeout [Seconds]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch>enable switch#configure switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch>enable switch#configure switch(config)# **8021x misc maxrequest 3**

8021x misc reauthperiod [Seconds]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch>enable switch#configure switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)#**8021x portstate authorize**
show 8021x	**P**	Displays a summary of the 802.1x properties and also the port sates.	switch>enable switch#**show 8021x**
no 8021x	**G**	Disable 802.1x function	switch>enable switch#configure switch(config)#**no 8021x**

Fault Alarm Commands Set

Netstar Commands	Level	Description	Example
fault-relay power [number] [enable/disable]	**G**	Configure Relay Alarm for Power Failure	switch>enable switch#configure switch(config)#**fault-relay power 1 enable**
fault-relay [enable/disable]	**I**	Configure Relay Alarm for Port Link Down/Broken	switch>enable switch#configure switch(config)#interface fastEthernet 1 switch(config-if)#**fault-relay enable**
show fault-relay	**P**	Show Fault Relay	switch>enable

		Alarm setting	switch#**show fault-relay**
no fault-relay	**G**	Disable Fault Relay Alarm function	switch>enable switch#configure switch(config)#**no fault-relay**

System Warning Commands Set

Netstar Commands	Level	Description	Example
systemlog mode [client|server|both]	**G**	Specified the log mode	switch>enable switch#configure switch(config)# **syslog mode both**
systemlog ip [IP address]	**G**	Set System log server IP address.	switch>enable switch#configure switch(config)# **syslog ip 192.168.1.100**
show syslog	**P**	Show SYSLOG configuration and log table.	switch>enable switch#configure switch#**show syslog**
no syslog	**G**	Disable systemlog functon	switch>enable switch#configure switch(config)#**no syslog**
smtp enable	**G**	Enable SMTP function	switch>enable switch#configure switch(config)#**smtp enable**
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch>enable switch#configure switch(config)#**smtp serverip 192.168.1.5**
smtp sender [sendername]	**G**	Configure sender of mail	switch>enable switch#configure switch(config)#**smtp sender test01**
smtp subject [subject]	**G**	Configure subject of	switch>enable

		mail	switch#configure switch(config)#**smtp subject alarm**
smtp authentication	**G**	Enable SMTP authentication	switch>enable switch#configure switch(config)#**smtp authentication**
smtp account **[account]**	**G**	Configure authentication account	switch>enable switch#configure switch(config)#**smtp account John**
smtp password **[password]**	**G**	Configure authentication password	switch>enable switch#configure switch(config)#**smtp password 1234**
smtp rcptemail **[Index] [Email address]**	**G**	Configure Rcpt e-mail Address	switch>enable switch#configure switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	**P**	Show the information of SMTP	switch>enable switch#**show smtp**
no smtp	**G**	Disable SMTP function	switch>enable switch#configure switch(config)#**no smtp**
event device-restart **[Syslog|SMTP|Both]**	**G**	Set device restart event type	switch>enable switch#configure switch(config)#**event device-restart both**
event authentication-failure **[Sysog|SMTP|Both]**	**G**	Set Authentication failure event type	switch>enable switch#configure switch(config)#**event**

			authentication-failure both
event syslog **[Link-UP|Link-Down|Both]**	**I**	Set port event for SYSLOG	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)#**event syslog both**
event smtp **[Link-UP|Link-Down|Both]**	**I**	Set port event for SMTP	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)#**event smtp both**
show event	**P**	Show event selection	switch>enable switch#**show event**
no event device-restart **[Syslog|SMTP|Both]**	**G**	Disable device restart event type	switch>enable switch#configure switch(config)# **no event device-restart both**
no event authentication-failure **[Syslog|SMTP|Both]**	**G**	Disable Authentication failure event typ	switch>enable switch#configure switch(config)#**no event authentication-failure both**
no event syslog	**I**	Disable port event for system log	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)#**no event syslog**
no event smpt	**I**	Disable port event for SMTP	switch>enable switch#configure switch(config)#interface fastethernet 3 switch(config-if)#**no event smtp**

Mac Address Table Commands Set

Netstar Commands	Level	Description	Example
show mac-address-table	**I**	Show MAC address table	switch>enable switch#configure switch(config)#interface fastethernet 2 switch(config-if)#**show mac-address-table**
show mac-address-table all	**P**	Show MAC address table (all)	switch>enable switch#**show mac-address-table all**
no mac-address-table	**G**	Remove dynamic entry of MAC address table	switch>enable switch#configure switch(config)#**no mac-address-table**
agingtime [seconds 0~3825 steps 15]	**G**	Configure mac address table aging time	switch>enable switch#configure switch(config)#**agingtime 30**
auto-flush [enable|disable]	**G**	Auto flush mac address table when ports link down	switch>enable switch#configure switch(config)#**auto-flush enable**

Port Statistics Commands Set

Netstar Commands	Level	Description	Example
show interface accounting	**I**	show interface statistic counter	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch (config-if)#**show interface accounting**

no accounting	**I**	Clear interface accounting information	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**no accounting**

Port Monitoring Commands Set

Netstar Commands	Level	Description	Example
monitor destination [RX|TX|Both]	**I**	Configure destination port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)# **monitor destination rx**
monitor source [RX|TX|Both]	**I**	Configure destination port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**monitor source rx**
show monitor	**P**	Show port monitor information	switch>enable switch#**show monitor**
show monitor	**I**	Show port monitor information	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**show monitor**
no monitor	**I**	Disable source port of monitor function	switch>enable switch#configure switch(config)#interface fastEthernet 2 switch(config-if)#**no monitor**

System Event Log Commands Set

Netstar Commands	Level	Description	Example
show syslog	**P**	Show SYSLOG configuration and log table.	switch>enable switch#**show syslog**

Ping Commands Set

Netstar Commands	Level	Description	Example
ping **[ip]**	**E**	Ping function	switch>**ping 192.168.16.1**

SFP Monitor Commands Set

Netstar Commands	Level	Description	Example
show ddm	**P**	Show temperature alarm information	switch>enable switch# **show ddm**

Loading Average Commands Set

Netstar Commands	Level	Description	Example
loadavg	**E**	Show system load average	switch>**loadavg**
event loadavg **[Systemlog|SMTP|Both]**	**G**	Set system load average event type	switch>enable switch#configure switch(config)# **event loadavg both**

Power over Ethernet Commands Set

Netstar Commands	Level	Description	Example
poe	**P**	Enter POE configure mode	switch>enable switch#**poe**
system knockoff-disabled **[Enable|Disable]**	**P**	Set PoE system Port Knockoff Disabled	switch>enable switch#poe switch(poe)# **system knockoff-disabled enable**
system ac-disconnect	**P**	Set PoE system AC	switch>enable

[Enable|Disable]		Disconnect	switch#poe switch(poe)# **system ac-disconnect enable**
system capacitive-detect [Enable|Disable]	**P**	Set PoE system Capacitive Detection	switch>enable switch#poe switch(poe)# **system capacitive-detect enable**
port [PortNumbers] **powerlimit** [Value]	**P**	Set Poe system Power Limit	switch>enable switch#poe switch(poe)# **port 1 powerlimit 11000**
port [PortNumbers] **state** [Enable|Disable]	**P**	Set PoE port State	switch>enable switch#poe switch(poe)# **port 1 state disable**
port [PortNumbers] **plfc** [Enable|Disable]	**P**	Set PoE port Power Limit from Classification	switch>enable switch#poe switch(poe)# **port 1 plfc enable**
port [PortNumbers] **legacy** [Enable|Disable]	**P**	Set PoE port Legacy	switch>enable switch#poe switch(poe)# **port 1 legacy enable**
port [PortNumbers] **priority** [Low|High|Critical]	**P**	Set PoE port Priority	switch>enable switch#poe switch(poe)# **port 1 priority high**
autoping enable	**P**	Set PoE auto-ping Enable	switch>enable switch#poe switch(poe)#**autoping enable**
autoping sendmail enable	**P**	Set PoE auto-ping Send Mail	switch>enable switch#poe switch(poe)# **autoping sendmail enable**
port [PortNumbers]	**P**	Set PoE schedule	switch>enable

schedule enable		Configuration	switch#poe switch(poe)#**port 1 schedule enable**
port [PortNumbers] **schedule day** [0~6] e.g.0=Sun,6=Sat **hour** [0~23] **power** [On|Down]	**P**	Set PoE schedule date day	switch>enable switch#poe switch(poe)#**port 1 schedule day 5 hour 21 power on** switch(poe)# **port 1 schedule day 0-1 hour 0-3 power on** switch(poe)# **port 1 schedule day 0,4 hour 0-3,5 power on**
show poe autoping	**P**	Show PoE auto-ping information	switch>enable switch#poe switch#**show poe autoping**
show poe schedule	**P**	Show PoE schedule information	switch>enable switch#poe switch#**show poe schedule**
show poe	**P**	Show Power over Ethernet information	switch>enable switch#poe switch#**show poe**

Save Configuration Commands Set

Netstar Commands	Level	Description	Example
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch>enable switch#**write memory**

Factory Default Commands Set

Netstar Commands	Level	Description	Example
default [keepip|keepadmin|both]	**G**	Restore to factory default configuration	switch>enable switch#configure switch(config)#**default both**

System Reboot Commands Set

Netstar Commands	Level	Description	Example
reload	**G**	Reboot switch	switch>enable switch#configure switch(config)#**reload**

Logout Commands Set

Netstar Commands	Level	Description	Example
logout	**E**	Logout command line shell	switch>**logout**